514.3

Security Policy Development and Assessment

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

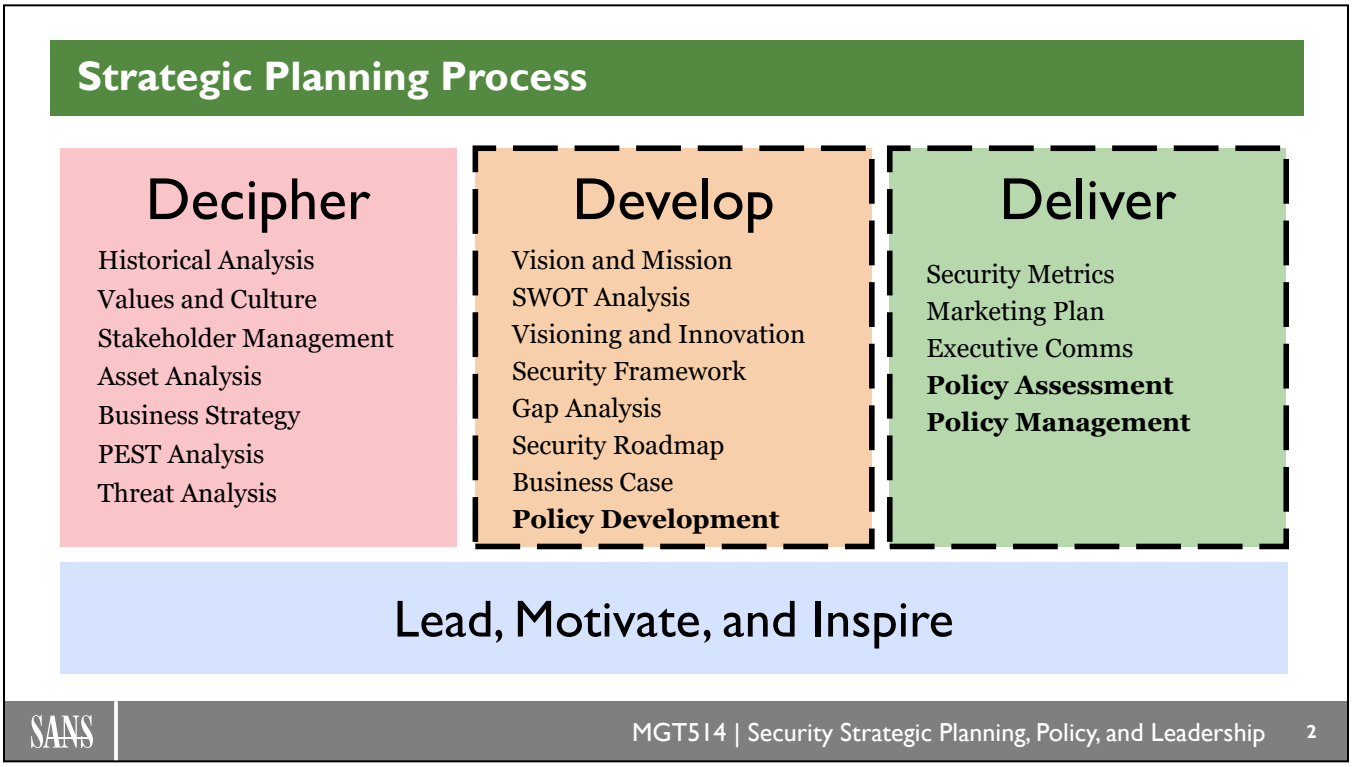
All reference links are operational in the browser-based delivery of the electronic workbook.

MGT514.3 | Security Strategic Planning, Policy, and Leadership

SANS

Security Policy Development & Assessment

Note about URLs
Sometimes, this courseware cites URLs that were valid at the time originally cited. URLs change all the time. This courseware does not necessarily update all URLs. Out-of-date URLs have several values. They show that a statement is based on scholarship. They can give hints about how to find source material even if it is no longer at the original URL. And they can be used to find material at the Wayback Machine maintained by the Internet Archive.



In this section, we focus on one of the most effective tools that we have as security leaders and managers to effectively steer the organization in a certain direction—security policy!

Security policies represent the stated risk appetite of the organization. As such, developing policy helps us execute and implement the items described in our security plan. Once policy is developed, though, we need to continue monitoring the business and threat landscape for any changes that require us to update policy. This is why our policy management, assessment, and audit capabilities are so important.

In Section 3, we cover the topics that are in **bold** on the slide above.

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- ***Purpose of Policy***
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

What Is Policy?

- Security Policy
  - Statement of goals from senior leadership
  - Defines expectations for how the security program, controls, and processes should be implemented
  - Documented approach for ensuring security and privacy of data
- Policy Set
  - Group of related documents that define an organization's security program
  - Planned, documented, and managed set of security controls
  - Includes policies, standards, guidelines, procedures, and baselines

At the highest level, policy is a statement from senior leadership that defines expectations for how the security program, controls, and processes should be implemented. For example, a high-level policy might define access only on a "need to know" basis. However, access is often associated with a password. As a result, we often refer to a "password policy" which contains more detailed information about complexity, length, expiration, and other factors. This is more detailed information that expands on the high-level policy of providing appropriate access.

So, security policy is better thought of as a general term that refers to any document that helps define an organization's security program. A "policy set" is a group of related documents that define an organization's security program. This policy set, which is sometimes referred to as a policy suite, can include not only policy documents but also standards, guidelines, procedures, and baselines. Keep in mind that there are different types, or levels, of "policy" documents. This includes the high-level policies themselves along with associated standards, guidelines, procedures, and baselines.

Purpose of Policy

- Protect people
  - Ensure safety from discipline if following policy and procedure
  - Establish the bounds of acceptable behavior
  - Empower people to do the right thing
- Protect the organization
  - Ensure data and systems are protected
  - Comply with regulations and laws

Organizations should adopt an umbrella policy so that to the extent possible, people should be able to work without fear. They should know that as long as they are following the policy, they are safe if something bad should happen. However, there is no substitute for the brain. They should also know that they are expected to use common sense.

One of the most important characteristics of policy is to establish bounds for behavior. Organizations typically have policies on a variety of subjects. What policies do organizations have that specifically relate to security? Identify what your organization does or does not have and try to make it better. Your actions may include lobbying to create or expand current policy. Without a security policy, any organization can be left exposed to the world. To determine your policy needs, you must first conduct a risk assessment. This may require an organization to define levels of sensitivity with regard to information, processes, procedures, and systems.

Policy Protects the Organization
Safeguarding information is a challenge when records are created and stored on computers. We live in a world where computers are globally linked and accessible, making digitized information especially vulnerable to theft, manipulation, and destruction. Security breaches are inevitable. Crucial decisions and defensive action must be prompt and precise.

A security policy establishes what you must do to protect information stored on computers. A well-written policy contains sufficient definition of "what" to do so you can identify and measure or evaluate the "how."

An effective security policy will help protect the company from legal and financial actions; however, it also has the effect of protecting people. Anyone who makes decisions or takes action in a situation in which information is at risk incurs personal risk, also. A security policy enables people to take necessary actions without fear of reprisal. Security policy compels the safeguarding of information while it eliminates, or at least reduces, personal liability for employees.

Policies are created by a company for protecting the company. Think of the policies your company has. Now, why were those policies created? Think about the reasons.

Most companies do not create policies because they think how useful it would be to have a policy that tells their users what is the acceptable way to do encryption. Most policies are created to address business and government regulations. Without these policies to guide the day-to-day actions of the company, the company opens itself to lawsuits, regulatory fines, and possible criminal prosecution.

Reasonable Person Rule

- When is it acceptable to not follow policy?
- Reasonable person rule takes into account:
  - The foreseeable risk of harm actions create versus the utility of actions
  - The extent of the risk so created
  - The likelihood such risk will actually cause harm to others
  - Any alternatives of lesser risk and the costs of those alternatives

The primary exception to policy protecting people is the reasonable person rule as codified by Justice Oliver Wendell Holmes, Jr. when he stated that it would not be reasonable to falsely shout fire in a theatre and causing a panic. While his statement was originally applied specifically to free speech not applying to someone who *falsely* creates a mass panic in a theatre potentially causing injury or even death, this concept can be applied to adherence to policy as well. In some cases, the foreseeable risk of harm in actually following policy might be greater than the risk of *not* following policy. If this risk is likely and could cause harm to others, it is reasonable to seek out alternatives that reduce risk.

References:
https://en.wikipedia.org/wiki/Reasonable_person
https://lsolum.typepad.com/legal_theory_lexicon/2003/10/legal_theory_le_3.html

Reasonable Person Example

- Captain Chesley "Sully" Sullenberger
  - Pilot who took unconventional action and saved 155 people
- Flight took off from New York's LaGuardia airport
  - Hit a flock of Canada geese, disabling both engines
  - Air traffic control advised returning to the airport
  - Sullenberger landed in the Hudson River instead
- To this day, multiple simulations have been run
  - None have been able to stretch the glide back to LaGuardia

Chesley Sullenberger is the pilot who took unconventional action and successfully landed an Airbus A320 in the Hudson River in New York City. Shortly after US Airways Flight 1549 took off from New York's LaGuardia airport for Charlotte, the plane hit a flock of Canada geese, disabling both engines. Several passengers saw the left engine on fire. Sullenberger had a conversation with air traffic control, and he quickly decided that landing in the Hudson River was the only option for everyone's survival. He landed the plane, with all 155 passengers and crew surviving, and to this day no simulations have been able to stretch the glide to return to LaGuardia. After landing in the Hudson, Sullenberger walked the unflooded part of the passenger cabin twice to make sure everyone had evacuated before retrieving the plane's maintenance logbook and being the last to leave the aircraft. Afterward, he said, "For 42 years, I've been making small, regular deposits in this bank of experience, education, and training. And, on January 15, the balance was sufficient so that I could make a very large withdrawal."

References:
https://www.vanityfair.com/culture/2009/06/us-airways-200906
http://www.huffingtonpost.com/2009/12/28/hudson-river-landing-pilo_n_404960.html

Bounds of Acceptable Behavior Example

No employee shall possess a hacking or monitoring tool unless authorized in writing for job-related reasons such as penetration testing.

How would you, as the security manager, feel if you found that an employee had a password-cracking tool on his or her machine? Without a policy statement pointing out this is beyond the boundaries of acceptable behavior, you might be able to warn the employee, but you might not be able to discipline. With such a policy in place, you would be able to enforce discipline. Disciplinary action may be taken, in accordance with HR policy, in addition to the issue-specific policy at hand.

Empower People to Do the Right Thing

- Facebook Responsible Disclosure Policy

> If you give us a reasonable time to respond to your report before making any information public and make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our service during your research, we will not bring any lawsuit against you or ask law enforcement to investigate you.

This policy appears to empower security researchers to do the right thing, but it also sets the boundaries of acceptable behavior. If policy states we can do something and procedures state how we can accomplish the tasks, we ought to do it without fear. This policy invites users to submit bug reports and is a good example of "positive voicing" combined with a thinly veiled threat.

Protect Data: Technology Disposal Example

When technology assets, PCs, laptops, pads, printers, copy machines, mobile devices, etc., have reached the end of their useful life, they should be sent to the local Information Technology office for proper disposal.

Information Technology will securely erase all storage mediums in accordance with current industry best practices.

We have all heard stories of organizations not realizing their copy machines had hard drives and failing to sanitize. Most users want to do the right thing; they just had no way of knowing the capability of something as simple as a copy machine or printer.

"Departments that are in possession of obsolete equipment will notify the Inventory Control department of the intent to dispose of said equipment and will complete a *Property/Asset Movement Request* form and obtain Dean, Director or Department Chair approval. Any theft of equipment must be immediately reported to CSN Police and documentation of this equipment is also done on a *Property/Asset Movement Request* form with appropriate approval."

Reference:
https://www.csn.edu/sites/default/files/documents/imported/equipment20disposal20policy.pdf (link no longer active)

Protecting PII Example

The Custodian must protect SSN and PII from unauthorized disclosure and access. In particular, as Legally Restricted Information, electronic copies of SSN must be stored only in designated data centers of the University or in another secure location, if authorized by a University Privacy Officer, or in encrypted or other secure form. Paper copies of SSN must be stored in locked rooms or cabinets. When a record containing a SSN or PII is no longer needed, it must be disposed of in a manner that makes the SSN unreadable and unrecoverable.

This University of Rochester policy is part of the university's efforts to deal with one of the biggest problems organizations face today: The loss of sensitive information. This often results in class action lawsuits, which are both expensive and distracting.

Reference:
https://tech.rochester.edu/wp-content/uploads/2015/09/SSN-PII-policy.pdf

Policy Protects Information

- Sample fragments

> Encrypt sensitive information during transmission
>
> Provide web access to customer information only through encrypted channels
>
> Encrypt business-critical files on mobile computers except while they are being edited
>
> There are only two types of information: That which is approved for public release and everything else

All of the items on the previous slide sound perfectly reasonable, and at first glance, they are, but good policy must also point to procedures that make these directives possible.

Employers who have sensitive data on their computer system—company plans, customer demographic data, or product designs—might need a clause in their security policy concerning trade secrets. Employees must clearly understand that under no circumstances should they pass proprietary company information through the internet unless it is encrypted.

Protect the Company: *New York Post* Privacy Policy

Some of the advertisements that appear on Post Sites are delivered to you by national internet advertising companies such as DoubleClick, Atlas DMT and 24/7 Real Media. These companies utilize certain technologies to deliver and select advertisements and marketing messages based upon anonymous information their technologies collect about your visit to Post Sites, including information about the banner ads they display, their cookie and your IP address. To opt out of information collection by these companies, or to obtain information about the technologies they use or their own privacy policies, please visit their websites.

The *New York Post* has a very well written and comprehensive privacy policy. This is just one fragment of it. Here, the company tells you that it collects marketing information as part of visiting its website. Interestingly enough, when I tested this site on March 26, 2013, the paper was using AdSonar, a different company than the ones mentioned. Privacy policies do help protect companies, but there is a gotcha: You need to do what your policy says and keep it up to date. This is potentially an example of a place where a more general policy might be suggested.

Reference:
http://nypost.com/privacy/

Protect the Organization: Comply with Laws and Regulations

- Review common legal, regulatory, and compliance frameworks
  - International
  - United States
  - European Union (EU)
  - China

A major reason we have a security policy is to protect the organization by helping it comply with various laws and regulations. In this section, we will cover a sampling of legal, regulatory, and compliance frameworks from around the world as an overview of the types of requirements that your organization might face as it does business domestically and internationally.

International: PCI DSS

PCI has 12 specific requirements designed to protect cardholder data and to prevent fraud

- Draft policies that address each of these domains within your organization
- Create policies that limit or prevent storage of credit card data and security codes
- Ensure your policies attempt to scope PCI environments narrowly and segment them from other IT systems
- Consider creating regulatory "agnostic" policies that cover requirements to the highest common denominator; then scope applicability accordingly

The Payment Card Industry (PCI) Data Security Standard (DSS) is not a law but rather a set of information security standards agreed upon by the major payment card companies (Discover, Visa, MasterCard, American Express, and so on).

Following is a list of the 12 DSS requirements:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Reference:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

United States: HIPAA

HIPAA is primarily focused on securing PHI

- Information Security policies of the Business Associate
- Information Classification Policies
- Policies governing the Administrative, Technical, and Physical Safeguards
- Mobile and Portable computer policies including encryption standards
- Policies requiring annual risk assessments and use of the Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) states that "A covered entity must adopt reasonable and appropriate policies and procedures to comply with provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments."

… A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI)."[1]

Numerous security policies need to be followed in order for a company to be HIPAA compliant when storing, processing, or handling protected health information.

If you are new to managing HIPAA-related data, consider the following policies, at a minimum, for quick adoption:

1. Ensure you are reviewing the security policies of the business associates with which you share e-PHI data annually.
2. Ensure you have an information classification policy so that you understand and have accurately classified e-PHI data wherever it resides in your organization.
3. Ensure you have policies in place that govern the Administrative, Technical, and Physical safeguards used to protect e-PHI and PHI data.
4. Specifically ensure you have security policies governing the use of mobile or portable computing devices, particularly focusing on encryption of the e-PHI data on those devices in transit and at rest.
5. Ensure you have security policies governing the process for conducting annual risk assessments and consider utilizing the HIPAA Risk Assessment tool.

The HIPAA Security Standards – Final Rule can be found here:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

The Security Risk Assessment Tool (SRA Tool) details can be found at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. The SRA tool provides 156 questions about the organization's activities and helps healthcare providers understand the Administrative, Technical, and Physical safeguards needed to properly protect e-PHI.

Reference:
[1] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

United States: SOX (Sarbanes-Oxley)

SOX is intended to provide policies enforcing ethical and honest accounting practices

- Auditing independence policies
- Clear data destruction and life-cycle policies
- Policies enforcing the rotation of independent third-party auditing firms
- HR policies preventing "whistleblower" retaliation
- Strong Duty to Monitor clauses
- Financial system logging and monitoring policies

SOX (Sarbanes-Oxley) is also known as the "Public Company Accounting Reform and Investor Protection Act" or the "Corporate and Auditing Accountability and Responsibility Act." In either case, the primary concerns for SOX are the accuracy and honesty of financial reports from publicly traded companies. With this in mind, potential security policies to consider drafting may include the following:

- Policies governing accounting practices
- Auditing independence policies
- Policies enforcing the rotation of independent third-party auditing firms
- HR policies preventing "whistleblower" retaliation
- Strong Duty to Monitor policy clauses
- Financial system logging and monitoring policies

SOX includes major controls in section 404 and 802 concerning internal IT controls and destruction of data, respectively. The entire law can be found at http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm.

Wikipedia summarizes the 11 major elements of SOX as follows:

1. Public Company Accounting Oversight Board (PCAOB): Title I consists of nine sections and establishes the Public Company Accounting Oversight Board to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

2. Auditor Independence: Title II consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (for example, consulting) for the same clients.

3. Corporate Responsibility: Title III consists of eight sections and mandates that senior executives take **individual responsibility** for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance. For example, Section 302 requires that the company's "principal officers" (typically, the Chief Executive Officer and Chief Financial Officer) certify and approve the integrity of their company financial reports quarterly.

4. Enhanced Financial Disclosures: Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance sheet transactions, pro forma figures, and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

5. Analyst Conflicts of Interest: Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

6. Commission Resources and Authority: Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, advisor, or dealer.

7. Studies and Reports: Title VII consists of five sections and requires the Comptroller General and the SEC to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

8. Corporate and Criminal Fraud Accountability: Title VIII consists of seven sections and is also referred to as the "Corporate and Criminal Fraud Accountability Act of 2002." It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations while providing certain protections for whistleblowers.

9. White Collar Crime Penalty Enhancement: Title IX consists of six sections. This section is also called the "White Collar Crime Penalty Enhancement Act of 2002." This section increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

10. Corporate Tax Returns: Title X consists of one section. Section 1001 states that the Chief Executive Officer should sign the company tax return.

11. Corporate Fraud Accountability: Title XI consists of seven sections. Section 1101 recommends a name for this title as "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freezing transactions or payments that have been deemed "large" or "unusual."

Additional U.S. Security and Exchange Commission reports on SOX can be found here:
https://www.sec.gov/news/studies/principlesbasedstand.htm

Reference:
https://en.wikipedia.org/wiki/SarbanesOxley_Act

California Privacy Rights Act (CPRA)

- Applies to any business in California that:
  - Has gross revenue of more than $25 million
  - Buys, receives, sells, or shares personal info of 100,000 or more consumers, households, or devices
  - Derives 50% or more of revenue from selling or sharing consumer personal info of CA residents
- Provides Californians right to:
  - Know what personal information is collected about them
  - Know whether their personal information is sold or disclosed and to whom
  - Say no to the sale of their personal information; limit use of personal information
  - Access their personal information
  - Equal service and price, even if they exercise their privacy rights
- Penalties
  - Damages of $100-$750 per consumer per incident, or actual damages
  - State can assess penalties of $2,500 for each violation or $7,500 for each intentional violation

The California Privacy Rights Act (CPRA) provides privacy and consumer protection for California residents. It enhances and effectively replaces the prior California Consumer Privacy Act (CCPA). The former went into effect on January 1, 2023, with enforcement starting on July 1, 2023. This is just three years after the prior CCPA went into effect on January 1, 2020. The CPRA is defined in Proposition 24[1] which was approved by voters and amends two prior bills

The California Consumer Privacy Act (CCPA) enhances privacy and consumer protection for CA residents. It was signed into law on June 28, 2018 and goes into effect on January 1, 2020. It is made up of two bills: Assembly Bill No. 375 (AB-375), which officially introduced CCPA, and Senate Bill No. 1121 (SB-1121), which included amendments to the original bill.[2]

CPRA applies to any business in California that meets one or more of the following conditions:

- Has gross revenue of more than $25 million
- Buys, receives, sells, or shares personal info of 100,000 (was 50,000 under CCPA) or more consumers, households, or devices of California residents
- Derives 50% or more of annual revenue from selling or sharing (this sharing part was added via CPRA) consumer personal info of California residents

The Act is grounded on the fact that privacy is defined as an inalienable right in the California Constitution. It provides Californians the right to:

- Know what personal information is collected about them
- Know whether their personal information is sold or disclosed and to whom
- Say no to the sale of their personal information
- Access their personal information
- Equal service and price, even if they exercise their privacy rights

The Act goes on to state that “any consumer whose nonencrypted or nonredacted personal information. . .is

subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action. . ."[3] Specifically, this includes seeking $100-$750 per consumer per incident or actual damages, whichever is greater as well as "Injunctive or declaratory relief" and "any other relief the court deems proper." Moreover, a civil penalty of $2,500 for each violation or $7,500 for each intentional violation can be assessed by a California Attorney General action.

CPRA also defines a Sensitive Personal Information (SPI) category which states that security measures should be appropriate for the following types of data:

- Social Security number
- Driver's license
- State identification card
- Passport number
- Financial account information and credentials
- Debit card or credit card number and corresponding access codes
- Precise geolocation data
- Religious or philosophical beliefs
- Ethnic origin
- Contents of communication
- Genetic data
- Biometric information
- Health information
- Information about sex or sexual orientation

Additionally, data retention periods must be defined and shared with consumers. Business must only retain personal information for as long as "reasonably necessary" for business purposes.

Unlike CCPA, which did not explicitly define who would be responsible for enforcement, the CPRA creates an exclusive enforcement agency called the California Privacy Protection Agency (CPPA). It is this agency that will determine if there is a "significant risk to its consumers' privacy or security", review the now required annual cybersecurity audits, and have a say in lawsuits, which can now also be brought for breaches of email address in combination with passwords or security questions/answers.

[1] https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf
[2] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375
[3] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

European Union: GDPR

EU General Data Protection Regulation (GDPR)

- Binding on:
  - EU member states
  - Members of European Economic Area (EEA)
- Applies to:
  - Any company that process data of EU citizens
  - Processing of personal data of subjects who are in the EU/EEA

The GDPR is effective as of May 25, 2018 and has been described as the "most important change in data privacy regulation in 20 years."[1] It is binding on all EU member states and members of the European Economic Area (EEA). It applies to any company that processes personal data of EU citizens. It also applies to processing of personal data of subjects who are in the EU/EEA. As a result, the GDPR has far-reaching, worldwide impact. Any company that has a customer from the EU or has a customer that visits the EU (and subsequently processes their data) must now comply with the GDPR.

The GDPR replaces the old Data Protection Directive (95/46/EC) which required member states to transpose this directive into various laws in those respective countries.[2] Now, the GDPR makes various data protection requirements mandatory and unifies data protection law across the EU by:

- Harmonizing 27 national data protection regulations into one unified regulation
- Improving user control of personal data
- Making it easier for businesses to work with a single Supervisory Authority (SA) as a "one-stop shop" for privacy complaints

Privacy complaints are adjudicated by data supervisory authorities or courts of member states with the closest relationship to the individuals in question or by the entities on both sides of the dispute.

References:
[1] https://www.gdpr.eu
[2] https://en.wikipedia.org/wiki/Data_Protection_Directive

European Union: GDPR Requirements

- Breach disclosure and penalties
  - Notification within 72 hours
  - Penalties up to 4% of global turnover or €20m
- Personal data requirements
  - Obtain customer consent to collect data
  - Describe what data is collected
  - Provide data in a portable format
  - Implement "right to erasure" and right to have data corrected
- Security program requirements
  - Implement "data protection by design and default"
  - Appoint a data protection officer (DPO)
  - Perform data protection impact assessments

The GDPR is a very comprehensive regulation that is over 250 pages in length. It is highly recommended to review the entire document to understand how it relates to your organization.[1,2] Here, we summarize a number of the most important GDPR requirements.

Breach notification within 72 hours (Article 34)
Organizations must notify their Supervisory Authority (SA) within 72 hours of becoming aware of a breach. Individuals must be notified if there is adverse impact "without undue delay." However, if data is anonymized or encrypted, the data subject does not need to be notified.

Penalties of 4% of global turnover or €20m (Article 83)
The penalties of up to 4% of global turnover or €20m (whichever is greater) can be quite severe. These penalties will depend, among other factors, on "the nature, gravity, and duration of the infringement", "the intentional or negligent character of the infringement", and "any action taken by the controller or processor to mitigate the damage suffered by data subjects."

Organizations must obtain customer consent to collect personal data (Article 7), describe what data is collected, provide personal data in a portable format (Article 20), implement a "right to erasure" (Article 17), and provide a mechanism to have data corrected. Companies must now implement security controls with "data protection by design and default" (Article 25). This means that companies can only use personal data that is necessary for the specific purpose. Organizations must also perform data protection impact assessments (Article 35) and appoint a data protection officer (DPO) per Article 37.

The Data Protection Working Party has published "Guidelines on Data Protection Officers" that describes the position and tasks of a DPO. Consult that for further reading on the responsibilities of your DPO.

References:
[1] https://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf
[2] http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

European Union: Privacy

- Trans-Atlantic Data Privacy (TADP) Framework
  - Allows data transfers from the EU to the US
  - Replaces the old Safe Harbor and Privacy Shield agreements
  - Requires US companies to meet and implement various requirements
- ePrivacy Regulation
  - Updated "cookie rule" to simplify notifications
  - Prohibiting spam emails

When doing business in the EU, there are also two important privacy-related frameworks to consider.

The Trans-Atlantic Data Privacy (TADP) Framework[1] allows data to be transferred from the EU to participating US companies. It replaces the both of the prior EU-US Privacy Shield[2] and Safe Harbor frameworks and requires US companies to attest to the fact that they meet various requirements outlined in the framework.

In 2013, Austrian lawyer Max Schrems filed a complaint against Facebook with the European Court of Justice with the aim of prohibiting the transfer of EU citizens' data to the US. Ultimately, it was ruled that the old Safe Harbor agreement for trans-Atlantic data transfer was invalid and that a new framework would need to be established.[3] This eventually resulted in the adoption of the new Privacy Shield agreement, which extends privacy protections to EU citizens and gives them access to US courts. In 2020 this was also deemed invalid (in a ruling referred to as Schrems II).

In addition to trans-Atlantic data transfer the EU also has requirements related to electronic privacy. The ePrivacy Regulation seeks to replace the existing ePrivacy Directive (Privacy and Electronic Communications Directive 2002/58/EC)[4] that protects privacy for online transactions.[5] The ePrivacy requirements are related to cookies used in web browsers to track user activity and to spam emails that may be sent to users. The "cookie rule" in particular has resulted in website notification messages describing the use of cookies to track user activity. The volume of cookie notifications has become problematic in some cases and the new regulation would likely simplify the way that cookie consent is tracked.

References:
[1] https://crsreports.congress.gov/product/pdf/IF/IF11613
[2] https://en.wikipedia.org/wiki/EU-US_Privacy_Shield
[3] https://en.wikipedia.org/wiki/Max_Schrems
[4] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation
[5] https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_Directive_2002

European Union: NIS Directive

- Directive on Security of Network and Information Systems
- EU member states must
  - Develop a national strategy on security
  - Designate a computer security incident response team (CSIRT)
  - Cooperate at a national level
- Digital service providers and operators of essential services are required to take appropriate technical and organizational measures
  - Security of systems and facilities
  - Incident handling and business continuity management
  - Monitoring, auditing, and testing
  - Compliance with international standards

The NIS Directive was adopted by the European Parliament and entered into force in August 2016. Member states had until May 2018 to transpose the directive into their national laws.[1]

The Directive requires member states to develop a national strategy on the security of network and information systems (including a governance framework), designate computer security incident response team (CSIRT), and cooperate at a national level.

The Directive also has articles that apply to digital service providers (e.g., online marketplaces, search engines, cloud computing providers) and operators of essential services (e.g., energy, transportation, finance, health, water, digital infrastructure). Organizations in these areas are required to take "appropriate and proportionate technical and organizational measures" that cover the following areas:

- Security of systems and facilities
- Incident handling
- Business continuity management
- Monitoring, auditing, and testing
- Compliance with international standards

Reference:
[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

China: Cybersecurity Law

- Penalties
  - Fines up to RMB 1,000,000
  - Suspension of business and cancellation of permits/licenses
- Data protection requirements
  - Personal information
  - Critical infrastructure
  - Security requirements for "network operators"
- Important data must be stored in China
- Certification of technology products

The Cybersecurity Law of the People's Republic of China was adopted on November 7, 2016 and went into effect on June 1, 2017.[1] Like other international laws, there is a focus on personal information protection (Articles 40-50) and critical infrastructure protection (Article 31), which includes "public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure."

The law also defines security requirements for "network operators" (Article 76). According to a KPMG document titled "Overview of China's Cybersecurity Law" the term "network operators" originally referred to network owners, managers, and network service providers.[2] However, this definition has been expanded to include "institutions that provide services and conduct business activities through networks" such as financial institutions, providers of security products and services, and enterprises with websites that provide network access. As a result, the scope of the Cybersecurity Law is very broad.

Failing to comply with the law can result in various penalties (Articles 64-66), including fines of up to RMB 1,000,000.

The law also requires data to be stored in China (Article 37) and states, "Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." There are fines of up to RMB 500,000 for violating data storage requirements as well as "temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses."

The Law also requires certification of technology products (Articles 23 and 35). It states that "Critical information infrastructure operators purchasing network products and services that might impact national security shall go through a national security review organized by the State network information departments and relevant departments of the State Council." Some, like Recorded Future, have argued that the Law gives "network information departments" overly broad power to conduct "national security reviews" that would require technology companies to submit source code or intellectual property for review before it can be sold in

China.[3] This puts foreign companies in a difficult decision of deciding whether they want to sell to the lucrative Chinese market or potentially have their intellectual property misused or analyzed for security vulnerabilities.

References:
[1] https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en
[2] https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf
[3] https://www.recordedfuture.com/china-cybersecurity-law/

Vendors and Third Parties

- How do you assess and select your vendors?
  - Third-party validation
    - SSAE (SOC 1, SOC 2 Type I and Type II)
    - ISO/IEC 27000 Series
  - Agreed-upon requirements
    - Trans-Atlantic Data Privacy (TADP)
    - Standard Contractual Clauses and Binding Corporate Rules
  - Assessments
    - Penetration testing results
    - Vulnerability scan results
    - Security program review

Security policies can be helpful as you seek to manage risks from third parties. Ensure you have security policies that define how you assess your vendors' policies and security posture. You may also want to strongly consider creating a vendor or third-party onboarding process in which your Vendor Management Office (VMO) or Purchasing department delivers a set of security requirements and business requirements for all bids and new products or services. Then, include that same language in your contracts with the vendors and ensure appropriate compliance testing is performed to validate the vendors are meeting the contractual obligations agreed upon.

It is also valuable to use the renewal periods when existing contracts or agreements will be extended, to renegotiate the security controls expected of all third parties and vendors or consider evaluating other vendors that meet your minimum-security standards.

When it comes to third-party assessments, consider the following available options:

Shared Assessments:
There are several recognized frameworks and assessment tools to help you with this effort. For instance, Shared Assessments is a framework developed and based on financial BITS security audits. This assessment relies on a Standard Information Gathering Questionnaire (SIG) and Agreed Upon Procedures (AUP). You can also purchase Shared Assessments SIG and AUP documents from https://sharedassessments.org.

SSAE (SOC 1, SOC 2 Type I and Type II):
In the accounting industry, the SSAE standards are used to measure controls of financial information. SSAE 18 has superseded SSAE 16 which had previously replaced the SAS 70 Type 1 and Type 2 assessments. More information about SOC 2 can be found at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

ISAE 3402 is a related assurance standard that is also used in conjunction with SSAE 16 and was developed by the International Auditing and Assurance Standards Board.

ISO/IEC 27000 Series:
ISO/IEC 27000 is a series of information security management standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that are designed to manage risks and security controls within an organization. ISO is used internationally and is recognized as a high-level bar for security certification. More information can be found at http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Standard Contractual Clauses and Binding Corporate Rules:
Standard clauses are plainly written common phrases that represent the current practice of the organization and are often used in contract negotiations. Large multinational organizations often use binding corporate rules to define rules within the company when transferring data to different divisions across national borders.

Strong Contracts:
Strong contracts are also an effective way to ensure security policies are enforced by vendors. Work with your Legal department, VMO, or Purchasing departments to ensure security requirements are clearly outlined in contract agreements with vendors storing, processing, or transmitting your confidential data. Also, ensure your contracts define how the vendor will provide evidence of compliance and potentially will grant your organization permission to test or audit these controls and policies.

Penetration Testing:
Penetration testing results can be a powerful indicator of cybersecurity risk and compliance to policies. Ensuring that your vendor(s) is conducting penetration tests or will allow your organization to do so, with written permission, can be an effective way to identify and prioritize security risks for remediation.

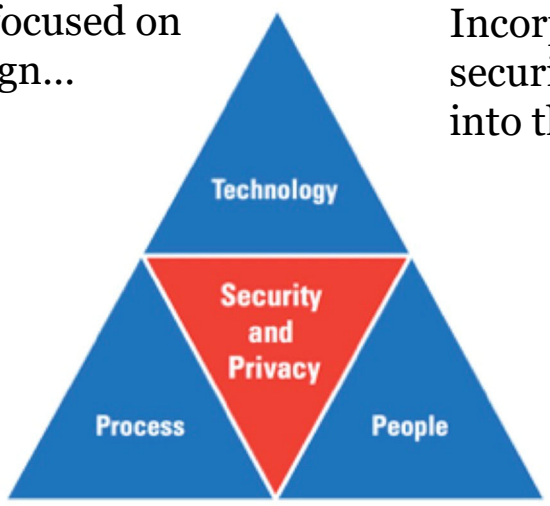
Vulnerability Scans:
Vulnerability scan results can also provide intelligence supporting a penetration test or can be used independently to identify how well a vendor is patching computer systems and applications. Vulnerability scans are only one indicator and should not be relied on exclusively. Compensating controls can often be used to mitigate vulnerabilities or can be claimed by vendors as risk management steps that should be confirmed through penetration testing.

Security Program Controls:
Security controls include, but are not limited to, applications and application development life cycles, infrastructure components controls, data center operations, change management processes, backup and recovery controls, and data protections, to name but a few. IT General Controls are defined by the Institute of Internal Auditors (IIA) in the Global Technology Audit Guide (GTAG) questionnaire, including 17 specific domains or topics. You can find more details on the website: https://en.wikipedia.org/wiki/ITGC

Other Considerations:
Other important tools for consideration with third parties or other internal departments within your organization include an annual review of data-sharing agreements, cyber breach insurance policies, and indemnification clauses with your third parties. All of these should be considered when signing agreements with others that will be provided access to your organization's sensitive data.

Compliance by Design

Policies should be focused on compliance by design…



Incorporating solid security practices into the culture.

Policies should focus on compliance by design, where the desired behavior of incorporating security best practices is woven into the culture of the organization. This includes the measurement components and reporting. Drafting policies to help your organization meet its obligations and add real value to the organization is a fundamental principle to take away from this section.

Developing comprehensive security policies includes understanding the business value, legal and compliance implications, and security program design. Other components of the compliance-by-design model ultimately focus on providing appropriate security and privacy controls in place to prevent breach, technology, people, and processes.

This model, in essence, implies the need for compliance by practice and not simply checkbox compliance.

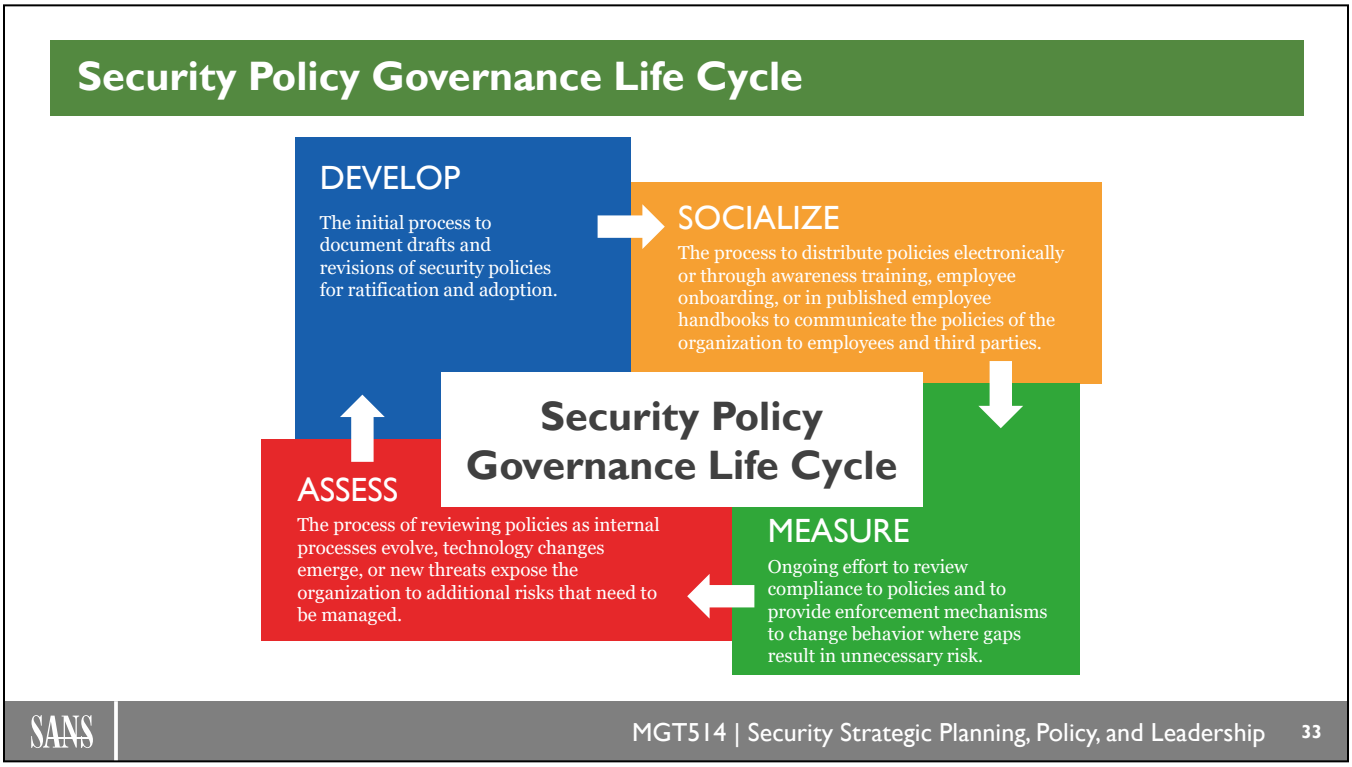
Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - ***Policy Pyramid***
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.



It is important to understand that creating security policies is really part of a life-cycle process. There are several discrete steps in the Security Policy life cycle:

1. **Develop:** The initial process to document drafts and revisions of security policies for ratification and adoption; this step includes identifying stakeholders such as business executives, legal counsel, the privacy office, and risk management teams. Keep in mind that no single stakeholder should dominate the process of developing or amending policies, but all stakeholders should be involved in the process.

2. **Socialize:** The process to distribute policies electronically or through awareness training, employee onboarding, or in published employee handbooks to communicate the policies of the organization to employees and third parties.

3. **Measure:** Ongoing effort to review compliance to policies and to provide an enforcement mechanism to change behavior when gaps are recognized between written policy statements and employee actions that cause unnecessary risk for the organization.

4. **Assess:** The process of reviewing policies as internal processes evolve, technology changes emerge, or new threats expose the organization to additional risks that need to be managed.

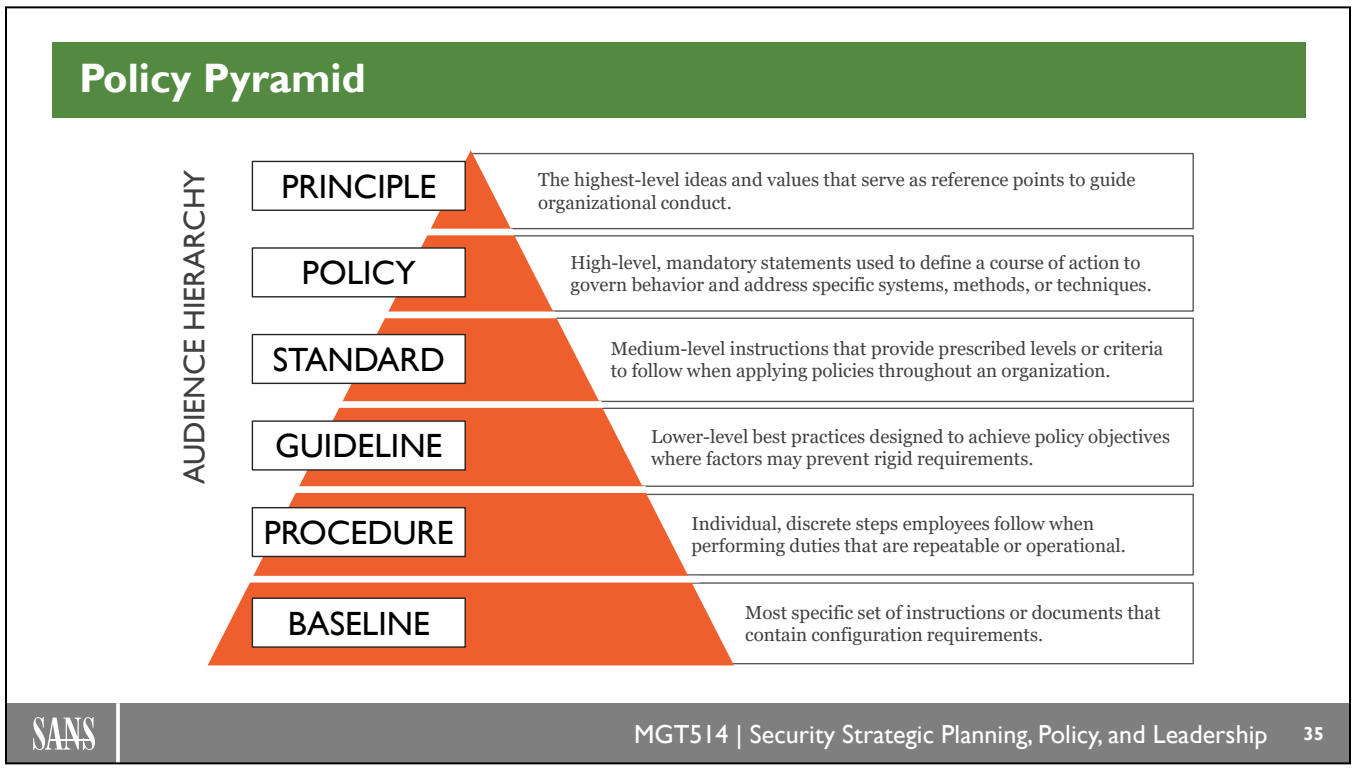
Other terms mentioned to describe the Security Policy life cycle may include Plan and Organize, Implement, Operate and Maintain, Monitor and Evaluate.

Reference:
http://searchsecurity.techtarget.com/tip/Steps-in-the-information-security-program-life-cycle

These same terms were also used in the COBIT 4 Governance life cycle applying to general IT systems and specifically, in this case, to IT policies.

Often, the full process to create and adopt a policy includes several tasks and subtasks. Some considerations may include the following:

1. Determine if a policy is needed.
2. Identify the stakeholders who should be involved.
3. Create a Tiger team of a few key members to draft the initial policy verbiage.
4. Submit the draft to the larger body for review.
5. Document changes.
6. Revise the draft.
7. Propose measurement and enforcement criteria for the policy.
8. Revise the policy if needed and resubmit for approval.
9. Document approval of the policy.
10. Measure and enforce the policy.
11. Review metrics with executives.
12. Review the policy annually for needed changes.



Every company has different terminology for the sets of instructions found in the policy pyramid.

One large, not-for-profit organization defined the policy pyramid with these terms. Smaller organizations may decide to use only a few of these instruction sets to govern organizational behavior.

Principles: The highest-level ideals and values that serve as reference points to guide corporate conduct. Principles provide the belief system backdrop for corporate decision making. Principles should describe the motivation behind a policy, the business benefit of utilizing the policy, or the cost, risk, or impact of not utilizing it. These are not policies in themselves, but rather they act as the foundation for thoughtful decision making and policy formation.

An example of a principle is when the company seeks to live the Golden Rule or to act and behave toward other customers, clients, or competitors in a way that is consistent with how we would want to be treated.

Policies: High-level, mandatory statements used to define a course of action to govern enterprise behavior. Policies provide direction for defining standards, guidelines, and procedures. Policies often include "must" and "shall" directives. Policies typically include several important components:

- Referential authority and accountability for the governing body enforcing the policy
- A focus on decision making and allocation of authority for decisions
- Are typically broad in scope and applicable to a wide audience
- Do not specify implementation details (for example, vendors, applications, or products by name)
- Include a policy steward, published and revision date, plus version control

An Acceptable Use Policy is an example that dictates how corporate internet resources shall be used for business purposes and usually specify types of websites that shall or shall not be visited during business hours.

Standards: Medium-level instructions that provide prescribed levels or criteria to follow when applying policies throughout an organization. Often, standards provide direction and help define specifications to meet the implied requirements of policies for specific systems, methods, or techniques. Standards typically include the following:

- Requirements defining rules
- Mandatory actions needed to comply or conform to a policy
- Details focused in a technology domain or discipline
- Requirements to apply to guidelines or procedural steps
- Revision dates and version control

For instance, a standard may state that all enterprise servers use a specific Windows or Linux operating system version.

Guidelines: Lower-level instruction statements of best practice designed to achieve policy objectives where factors may prevent a rigid requirement. Often, guidelines use the directives "may" or "should" to specify desired behavior. Guidelines influence but do not dictate decision making and should be followed despite the absence of a direct or specific mandate when possible. Guidelines typically include the following:

- Guideline author and authority
- Recommendations to be implemented
- Revision dates and version control

An example of a guideline could be for hard drive data destruction. There may be multiple ways to safely destroy the data on a hard drive, but some options may be more expensive or effective than others. The guideline specifies the preferred methods.

Procedures: The individual, discrete steps employees are intended to follow when performing duties that are repeatable or of an operational nature. For instance, in a server component assembly job where managing static electricity is a high priority, the process for inserting computer parts like the RAM, CPUs, voltage regulators, and other computer components should include a procedure for discharging static electricity, using an antistatic mat and an antistatic wrist strap during the installation process. Procedures typically include the following:

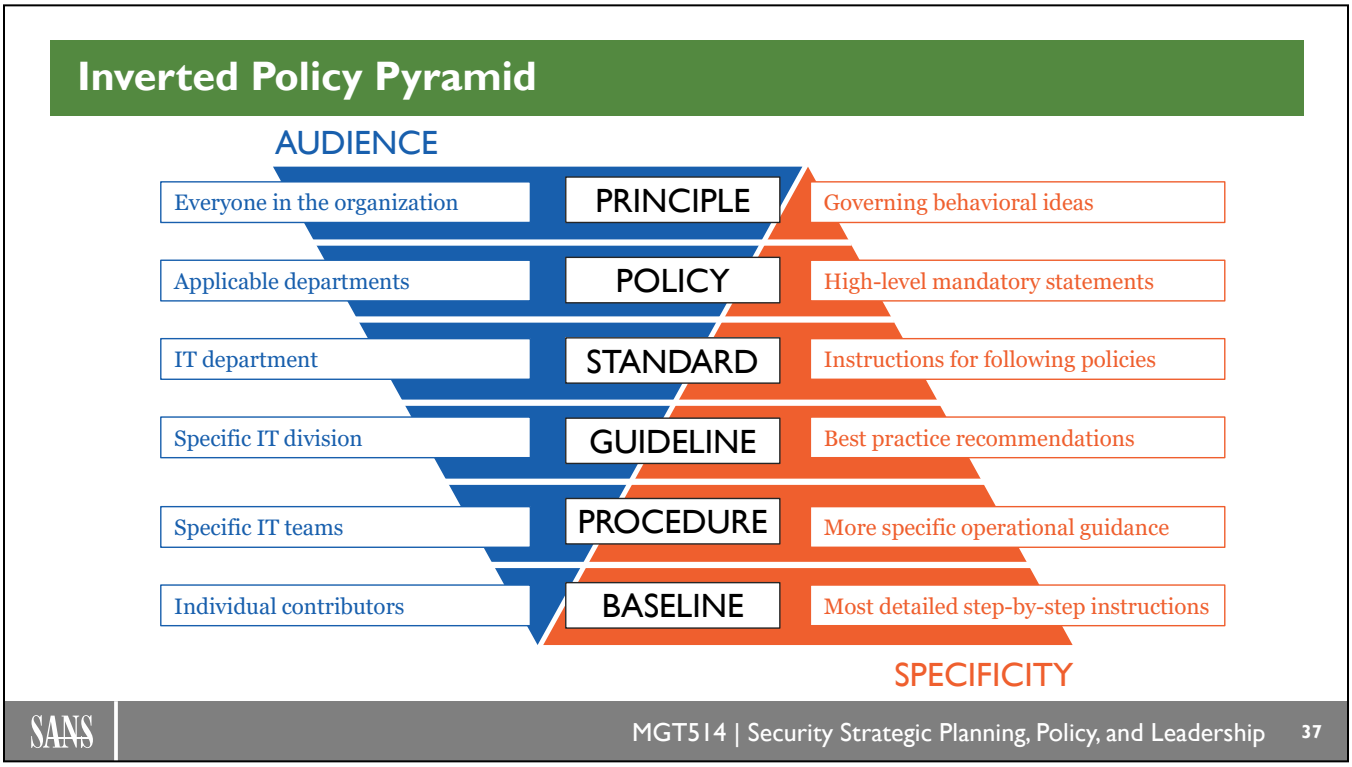
- Procedure author, authority, and technologies in scope
- Procedures to be implemented
- Revision dates and version control

This example of a procedure includes more details, steps, or a "run book" to follow to assemble the hardware before installing the operating system on a new server.

Baselines (or benchmarks): The most specific set of instructions or documents that contain configuration requirements for domain-specific technologies, including settings and parameters for individual platforms, applications, standard service offerings, or infrastructure. Baselines typically include the following:

- Baseline author, authority, and detailed technologies in scope
- Precise step-by-step instructions to be implemented
- Revision dates and version control

For example, a configuration baseline may include additional details for server hardening above and beyond the details specified in the server operating system standard. Procedures may also be included in the baseline, but typically the baseline is the most detailed of all the policy pyramid instruction sets.



The inverted Audience (People) specific pyramid reflects the concept that in an organization, instructions are intended for all employees in a descending manner because the requirements are more specific to the employees responsible for the function or task to be completed. For instance, the executive team and board of directors are heavily involved in creating and evangelizing the principles of the company, and these principles universally apply to all.

The policy committee, privacy office, and other stakeholders then act on those principles and under the direction of the board to draft policies to govern employee behavior at a high level through policies and standards.

In each successive step down the policy pyramid, additional middle management and end-line employees play an important role in defining the procedures, guidelines, and baselines as the tasks get more team, individual, or task focused.

Similarly, the Specificity (Details) triangle shows a hierarchical relationship that is ascending. At the bottom of the triangle are the baselines, the most detailed and specific instructions needed in the organization. In each ascending level, the instructions get progressively broader and less technical. For clarity, the short phrases on the next page briefly describe each component.

Audience:
Principle: Everyone in the Organization
Policy: Applicable Departments
Standard: IT Department
Guideline: Specific IT Division
Procedure: Specific IT Teams
Baseline: Individual Contributors

Specificity:
Principle: Governing Behavioral Ideals
Policy: High-Level Mandatory Statements
Standard: Instructions for Following Policies
Guideline: "Best Practice" Recommendations
Procedure: More Specific Operational Guidance
Baseline: The Most Detailed Step-by-Step Instructions

It is not uncommon for principles to be included in policies and standards in the form of noncommittal statements lacking the "must" or "shall" language. Generally, they are used in large, mature organizations, but they do not typically stand on their own without the supporting policies, standards, and so on. Principles can also be closely related to mission statements and other similar behavioral ideals.

Creating Effective Security Policies

1. Create policies that reduce risk to the organization, not increase liability
2. Socialize and educate employees about policies
3. Measure and enforce compliance by publishing results on your security dashboard
4. Regularly assess and update policies

Keep in mind that security policies should align directly with business goals and risks.

Four basic steps are needed to create effective security policies:

1. Create policies that reduce risk to the organization, not increase liability. Ultimately, this means you need to ensure your policies are achievable and tailored to the business. It is also very important to identify the applicable legal, contractual, or regulatory controls for your industry so that you can customize your policies to manage these obligations. In addition, helping your executives and the board of directors understand their "Duty to Monitor" will go a long way toward building an effective security policy and compliance program.

2. Socialize and educate employees about your policies. Employees need to understand where to find the security policies and to understand what they say so that they have real value to the organization. Create an easy and effective mechanism for socializing your policies with all of the employees in multiple ways so the policies help reduce risk to the organization.

3. Measure and enforce compliance by publishing results on your security dashboard. It is very important to measure how well your policies are being followed and to ensure effort is taken to correct behavior when policy violations are discovered. Using a security dashboard or Gemba board is critical to provide visibility of policy compliance and to build value for the policy and compliance programs. More details about the Gemba board will be covered in the metrics and dashboard sections of the course.

4. Regularly assess and update policies. As you measure compliance, review regulatory changes, and re-evaluate your business needs, you will need to update policies so they help you manage risks effectively. Policies should be reviewed and potentially updated annually, after completing risk assessments or whenever significant regulatory or security events dictate.

Creating policies can be a time-consuming process. Start with the policies you believe will reduce the greatest amount of business risk to the organization. If you are just starting with this process, look for policy frameworks that you can adopt over time.

Many examples of policy frameworks are readily available, such as the one provided by the UK government: https://www.gov.uk/government/publications/security-policy-framework

SANS also has a set of security policy templates that you can use to get started: http://www.sans.org/security-resources/policies/

Policies Should Reduce Risk

- Develop policies that reduce risk to the organization, not increase liability
  - Identify your policy obligations
  - Draft policies using simple language
  - Make sure policies are achievable
  - Ensure you can measure compliance
  - Remember, policies should not reflect a future maturity state
  - Help the board understand their "Duty to Monitor"
    - From the Caremark legal case

One of the most important steps to take to reduce risk to the organization is to draft security policies that align with the applicable legal, contractual, or regulatory controls for your industry. As you better understand the environment you are working in, you will be able to prioritize the adoption of security policies that reduce the greatest risks. More information about this concept will be presented on the next slide.

It is also important to keep in mind that security policies should be easy to read and written using simple and familiar language. Ensure translation of your policies is available in international offices or whenever needed.

Remember to use policy language that gives the organization some flexibility when interpreted by a regulator or auditors where possible. Focus on using language in policies that implies your organization is working to meet the "Due Care" standards expected in the industry. Use words such as "strive," "endeavor," or "seek" in policies when describing the organization's desire to avoid breach and when speaking about policies that are designed to protect customer and corporate data. Breach is almost inevitable, so ensure your policies are balanced.

It is equally important to make sure that for every policy you create, you need to have a Policy Steward assigned ownership to settle disagreements and to maintain the relevance of the policy.

Draft policies that you can implement throughout the organization. Policies that cannot be followed introduce additional liability to the organization. Work with legal counsel and executives to reconcile discrepancies between the policy obligations and the compliance capabilities of the organization. This effort will lead to additional transparency and likely a prioritization of policies that are needed and funding for technologies to enable these policies.

Ensure that for each policy you draft, you create a way to measure compliance for the policy. Plan to automate your compliance measures over time so they do not become unmanageable.

Policies should reflect the current state of maturity in the organization. Security professionals should use extreme caution when trying to write overly prescriptive or unobtainable policies in an effort to steer the organization in the right direction. Usually, it is better to have fewer policies that you can actually follow and measure and then add additional policies as needed as the organization matures.

If you are struggling to get executive support for your policies, help the board and executives understand their "Duty to Monitor" obligation. "The Duty to Monitor under Delaware Law: from Caremark to Citigroup" is an excellent paper that discusses the risk management duty of executives, boards of directors, and their personal obligations to monitor "corporate acts." In essence, the executives must be aware of the corporate policies and compliance with these policies and they must take action whenever they discover that policies are not being followed appropriately. We will discuss more about the Duty to Monitor in the next few slides.

If you are struggling to get the executive support you need, gather recent *Wall Street Journal* articles about board of director responsibilities to monitor and govern the companies they lead.

The general takeaway is to have policies that reduce risk and not incur additional risk if they are not practical.

Duty to Monitor (1)

"...A careful balance must be struck between the encouragements of entrepreneurial risk taking to grow the business and exploit new opportunities, on the one hand, and, on the other, the need for the board to ensure that those risks are taken in an appropriate and reasoned manner."

- Eric J. Pan

The 1996 Delaware Chancery Court decision, In re Caremark International Inc. Derivative Litigation, hereafter "Caremark," is a lawsuit filed by the shareholders alleging that the company's directors were negligent in their stewardship for failing to install and operate adequate policies and compliance programs to monitor for fraudulent or criminal behavior by the employees. As a result, the company faced substantial fines and civil penalties that could have been avoided if the board had taken reasonable precautions. The Caremark case and subsequent legal decisions have solidified the requirement that corporate directors (for example, Boards of Directors and Executive leadership) have a responsibility to adopt and maintain corporate compliance programs designed to detect and alert them of wrongdoing.

Eric J. Pan drafted the Duty to Monitor quote found in the Director Notes, "The Duty to Monitor under Delaware Law: from Caremark to CitiGroup," published in The Conference Board, February 2010, no. db-004 https://www.conference-board.org/publications/publicationdetail.cfm?publicationid=1742

This quote emphasizes the need for the board of directors to be aware of the risks the organization is taking, monitoring and providing governance and appropriate oversight. This includes the Fiduciary Duty to Monitor in addition to the Duty of Good Faith, which implies reasonable oversight and governance across the organization.

"Eric J. Pan is associate professor of law at the Benjamin N. Cardozo School of Law in New York. He received a J.D. from Harvard Law School and an A.B. from Harvard College."

Duty to Monitor (2)

"Caremark shifted the burden onto boards to put in place and evaluate the adequacy of its internal control and information reporting systems and to take into consideration the legal and economic environment of the corporation."

- Eric J. Pan

As financial risks have evolved from primarily fraud-based risks to more sophisticated cybersecurity breach risks, the Duty to Monitor has expanded also to include board involvement in adopting and enforcing cybersecurity policy to manage risks appropriately. This is a healthy change that should lead to better-managed organizations and fewer Enron debacles.

In that respect, the Duty to Monitor is one of the most important tools security practitioners can use to remind executives and boards of directors of their obligation to oversee the activities of the business with a watchful eye and to ask hard questions about governance and cybersecurity of corporate data and systems.

"The Duty to Monitor under Delaware Law: from Caremark to CitiGroup," published in *The Conference Board,* February 2010, no. db-004
https://www.conference-board.org/publications/publicationdetail.cfm?publicationid=1742

Also see Jill E. Fisch, "Taking Boards Seriously," *Cardozo Law Review*, Volume 19, 1997, p. 267.

The CVS/Caremark logo: https://www.caremark.com/wps/portal

Create Policies for Your Business

1. Identify the applicable legal, contractual, or regulatory controls for your industry
   - PCI - DSS
   - HIPAA/HITECH
   - GLBA
   - SOX
   - FFIEC
   - FERC / NERC
   - GDPR
   - ePrivacy

Many organizations must comply with legal, contractual, or regulatory controls to protect sensitive information. It is advisable to always check with legal counsel to determine what your organization's regulatory and legal obligations are. Keep in mind that not all regulations are equally prescriptive. Some obligations are very prescriptive, such as the PCI DSS. Others leave more discretion in control selection and implementation, such as the HIPAA Security Rule. Some organizations face a long, steep path to reaching a substantially compliant position. In these situations, leadership may consider outsourcing functions that are in-scope for regulation to qualified and experienced service providers who can demonstrate compliance through third-party audit attestations.

Common regulations to consider in your security policies may include but may not be limited to the following:

Health/Medical:
HHS (http://www.healthit.gov/policy-researchers-implementers/hipaa-and-health-it)
HIPAA (Health Insurance Portability and Accountability Act of 1996)
FDA 21 CFR Part 11
HiTECH

U.S. Federal Government:
FISMA (Federal Information Security Management Act of 2002)
NSA guidelines
NIST standards
Clinger-Cohen Act
Computer Security Act of 1987
U.S. Government Performance and Results Act (GPRA)
U.S. Government Paperwork Elimination Act (GPEA)
Toxic Substances Control Act of 1976 (TSCA) and TSCA Modernization act of 2015

Infrastructure, Energy, and Chemical:
FERC and NERC Cybersecurity Standards
Chemical Sector Cyber Security Programs
NIST Cyber Security Framework
Department of Energy Framework for SCADA Security Policy
(http://energy.gov/sites/prod/files/Framework%20for%20SCADA%20Security%20Policy.pdf)
ICS-CERT Common Industrial Control System Vulnerability Framework
(https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG)
American Chemistry Council – Chemical Sector Cyber Security Program
(http://www.chemicalcybersecurity.com)

Financial Services:
Sarbanes-Oxley Act (SOX)
Gramm-Leach-Bliley Act (GLBA)
PCI-Data Security Standard (PCI-DSS)
SAS 70
SSAE 16
U.S. Securities and Exchange Commission (SEC) 10-K Filings (http://www.sec.gov/answers/form10k.htm)
BITS Software Assurance Framework

International Security Frameworks:
IEC/ISO 17799:2005
IEC/ISO 27002
Committee of Sponsoring Organizations of the Treadway Commission (COSO)
(https://www.coso.org/pages/guidance.aspx)
Control Objectives for IT (COBIT) V.5
(https://www.isaca.org/resources/cobit)

LAW:
State, federal, EU, international law
Chapter 8 of the U.S. Sentencing Guidelines
MA State Law CMR 17.00
CA SB 1386

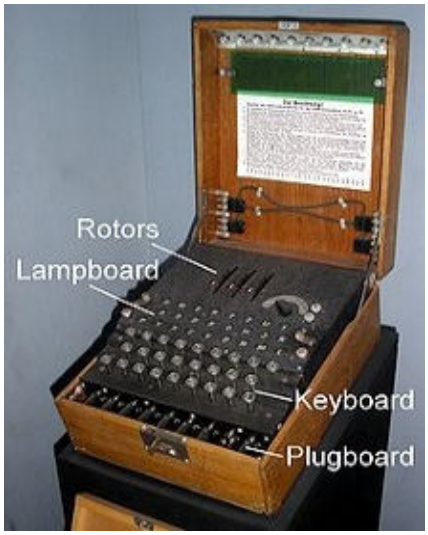
Others:
Organization for Economic Co-operation and Development (OECD) Policies

The PCI DSS-compliant graphic was found at https://www.pcicomplianceguide.org/.

Policies Should Encourage Employees to Behave Appropriately

German Enigma Example

- Policies and procedures were documented
- When they were followed, highly secure communication
- When not followed, significantly contributed to the outcome of the war



The German Enigma machine is a prominent example of how critical policies and procedures can be to a mission or cause. The Enigma machine, although there were several different varieties, generally used a daily, rotating cipher key that transformed the German Morse-Coded radio messages into ciphertext that needed to be decrypted in order to be translated and then read by the Allies. This rotating key limited the amount of time the Allied cryptanalysts could attempt to decipher messages being sent across German radio waves by identifying common phrases and word patterns in standard radio reports.

German policies and procedures may have been drafted to ensure this daily key was rotated to maintain the secrecy of the encryption algorithm, but failure to follow this policy with consistent regularity is the primary factor attributed with breaking the Enigma encryption. It is commonly believed that this policy failure and its subsequent exploitation by the Allies ended the war two years earlier than expected.

References:
Welchman, Gordon (1997) [1982], *The Hut Six Story: Breaking the Enigma Codes*, Cleobury Mortimer, England: M&M Baldwin
Calvocoressi, Peter (2001) [1980], *Top Secret Ultra*, Kidderminster, England: M&M Baldwin

A recent film, *The Imitation Game* (2014), is a historical thriller based loosely on the biography of *Alan Turing: The Enigma,* which describes the Axis policy and procedural failures leading to the breaking of the Enigma.

Image source: https://en.wikipedia.org/wiki/Enigma_machine

Organizational Adoption

2. Socialize the policies with everyone in the organization
   - Ensure the executives support the policies and are willing to comply themselves
   - Distribute the policies in multiple venues
     - Intranet sites
     - Printed materials or signage in break rooms/cafeterias
     - Via security or policy awareness training
     - During employee compensation review cycles
   - Align policies with your enterprise risk plan

Organizations with the most success implementing security policy and compliance programs are those that have executive support for and compliance with the policies themselves. It is critical that the executives and the board of directors are personally willing to follow the policies, or support at lower levels of the organization will be difficult to obtain and retain. After you get leadership on board with the policy and compliance program, then you must move your message down the corporate ladder.

To ensure policies are followed, you must ensure they are easily found, easily read, and well understood. To do this, ensure you distribute policies in multiple venues throughout the company. For instance, simply storing them on your intranet page may not be sufficient. You may also want to engage your marketing team to come up with creative ways to get the message across. This effort may include embedding the policy content in the annual security awareness training, posting signs in break rooms or the cafeteria, or requiring employees to read and agree to abide by the updated materials during the annual review process when performance bonuses and merit increases occur.

Additionally, you may want to make banners, posters, or other signage to hang throughout the buildings whenever significant policy changes are codified to alert employees of the changes. Some companies even resort to gamification and other tactics to encourage employees to familiarize themselves with policies. The more effort executives take to communicate the security policies of the organization, the more evidence they will have to show that they were earnestly striving to meet the "Due Care" standards if a breach ever occurs.

Highly mature organizations often find value in aligning security policies with the enterprise risk plan. An enterprise risk plan is typically a list of the most mission-critical applications, systems, business processes, or intellectual property that has the greatest need for protection and security. This focus will help to drive home support for the security policies that most directly improve the security of the most important business risks for the organization.

Measure and Enforce Compliance

3. Enforce policies throughout the organization uniformly
   - Ensure each policy follows the SMART model and can be measured
   - Work with HR and leadership on enforcement so your policies are not paper tigers
   - Manually gather results and create reports
   - Work to automate the process over time
   - Ensure executives get the message

Enforce policies throughout the organization in a uniform way.

Ensure each policy follows the SMART model and can be measured. The SMART model will be discussed in greater detail later in the course.

As policies are adopted and socialized, it is very important that the policies are enforced uniformly. This is particularly true when a significant policy violation has occurred. For instance, if employees consistently ignore policies that put the security of the entire organization at risk, it is important to have solid relationships with the HR department so that the behavior can be managed appropriately and consequences are appropriate. Without enforcement, policies often do not reduce business risk; they increase it. Of course, self-assessment and peer enforcement methods are far more effective at building mutual trust with and respect for the Security department than HR intervention.

Manually gather results and create reports. Use the computer systems you have at your disposal to generate reports monthly, quarterly, or whatever the duration specified in the policy. The policy steward may be tasked with this responsibility, or it may be delegated to another department. Whoever has the responsibility, ensure it is done regularly.

Work to automate the process over time and retain the information in a Governance, Risk, and Compliance (GRC) database or an equivalent for your organization.

Ensure executives get the message. This is perhaps the most important step of them all. If the executives do not receive the information about the policy and compliance results, significant business risks can be overlooked. This puts the executives at risk, in addition to security practitioners, for not making this message as transparent as possible. This is where the security dashboard should come into play. We will discuss more about the security dashboard later in the course, but we cannot state enough that the power of peer pressure when displaying metrics on a dashboard will be one of the single most important tools you can use to improve the security posture of the organization.

The SMART graphic was originally found at http://conversationalmarketinglabs.com (Historical reference - link no longer active)

Update Policies Regularly

4. Regularly meet with the stakeholders for each of the policies in the organization
   - Conduct an annual review of each policy with the policy steward and other stakeholders
   - Review the compliance criteria and risks the policy is designed to manage
   - Reassess changing legal and privacy implications
   - Adjust the policies accordingly

Regularly meet with the stakeholders to review and potentially update each of the policies in the organization. The policy steering committee or other policy sponsors, business executives, legal counsel, privacy officers, and policy stewards should be included to ensure they have an equal stake in the process.

During this annual review of each policy, determine if computing, technology, legal, risk, or privacy implications warrant changes to the policy. Keep in mind that no single stakeholder should dominate the process of developing or amending policies.

Review the compliance criteria and risks that the policy is designed to manage. If the changes are necessary, ensure they ultimately will help the organization reduce risk.

Reassess changing legal and privacy implications so that the organization is responsive to new laws and requirements for doing business around the globe.

Adjust the policies accordingly as new information becomes available while keeping the policies worded so that they are achievable and measurable.

Policies and Risk Assessments

- Policies should require risk assessments
  - Assessment results should drive policy
- Risk assessment approaches
  - Quantitative Risk Assessments
    - Objective assessments typically quantified using monetary values of risk
  - Qualitative Risk Assessments
    - Subjective assessments generalizing more broad levels of risks
    - Low, Medium, High
  - Hybrid Risk Assessments
    - A combination of both quantitative and qualitative risk assessment methods

What is a risk assessment? A simple definition of a *risk assessment* is the process of reviewing an asset and then identifying the threats to that asset and the controls in place to protect the asset from attack or compromise. Many types of risk assessments are used in different industries. This includes the identification, evaluation, and estimation of the risks involved in a situation, their comparisons against benchmarks or standards, and determination of an acceptable level of risk.

Quantitative Risk Assessment is the use of measurable, objective data to determine asset value, probability of loss, and associated risk which is often expressed in monetary terms. Douglas Hubbard has written two books, *How to Measure Anything: Finding the Value of Intangibles in Business* and *The Failure of Risk Management: Why It's Broken and How to Fix It* that provide foundational research for the use of quantitative methods.

Qualitative Risk Assessment is the use of relative risk rankings using descriptive categories such as low, medium or high or scales such as 1 to 10.

The terms “quantitative” and “qualitative” imply an either-or choice. In reality, it is very difficult to conduct a purely quantitative risk analysis because the measurements are applied to qualitative properties. Additionally, organizations that have been using qualitative approaches often have difficulty adopting quantitative methods. It is more appropriate to consider the degree to which analysis is based on quantitative and qualitative methods and how a hybrid approach can be used to better manage risk.

Encourage Employees to Obey the Law

- Know the laws by which you are governed
- Engage your Privacy Office
- Work with your attorneys or legal counsel
  - Understand statutes
  - Case law
  - Federal law
  - International considerations

Policies should strongly encourage employees to obey the law. Often, in the court of public opinion, it is very important that policies encourage employees to do the right thing and to meet minimum "Due Care" standards. Often, internal policies are disclosed to the public through lawsuits, news media coverage, or when posted online by disgruntled employees. Ensure your policies encourage behavior that is both legal and ethical.

Know the laws you are governed by. Work with your Privacy Office and legal counsel to clearly articulate the laws and legislation that govern business transactions or activities in the jurisdictions where you operate. Laws are constantly changing or becoming more specific, so it is imperative that these constant changes are integrated into your policy development life cycle.

In summary, ensure you are working with the appropriate stakeholders to understand relevant statutes and case law and you are incorporating this information into your policies. Also ensure you are monitoring compliance with policy and you can provide evidence you are trying to follow them; otherwise, don't have them.

This page intentionally left blank.

CYBER42

Event #7
Debrief

This page intentionally left blank.

Resources

- SANS Security Policy Templates
  - Free sample documents created by the security community
- *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*
  - By Douglas J. Landall
  - Example checklists, sample policies and procedures, and guidelines
- *Information Security Policies Made Easy*
  - By Charles Cresson Wood
  - Thirteen editions published since it was first written
  - Over 1,500 prewritten policies that map to various compliance regulations

A number of policy-related resources are available online.

SANS Security Policy Templates:
Free templates created by contributions from the security community covering a variety of security-related topics.
https://www.sans.org/security-resources/policies

Information Security Policies, Procedures, and Standards: A Practitioner's Reference:
Information on how to develop effective security policies and procedures with example checklists, sample policies and procedures, guidelines, and information on applicable standards.
https://www.amazon.com/Information-Security-Policies-Procedures-Standards/dp/1482245892

Information Security Policies Made Easy:
Commercial publication written by Charles Cresson Wood that contains hundreds of prewritten policies that can be used as a starting point for your organization.
https://www.rothstein.com/product/information-security-policies-made-easy

Types of Policies to Have in Your Organization

- Governance
  - Information Security Program
  - Data Classification and Handling
  - Security Roles and Responsibilities
  - Risk Management, Vendor Risk
  - Training and Awareness
  - Business Continuity, Disaster Recovery
  - Change Control
- Operational
  - Server, Network, Firewall
  - Information Handling and Disposal
  - Patching/Vulnerability Management
- Security
  - Authentication, Access Control, Password
  - Physical Security
  - Personnel Security
  - Incident Response
  - Security Review and Audit
  - System Development Lifecycle
  - Logging and Monitoring
  - Data Protection
- Acceptable Use
  - Email, Internet, Social Media
  - Remote Access, Mobile, Cloud

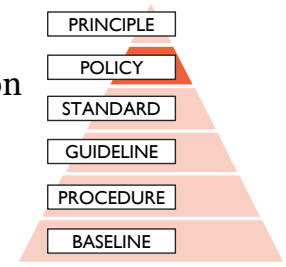
These are examples of security policies that you should have in your organization.

Placing security policies into one of the four categories above aids in policy development, socialization, and communication. For example, policies in the Governance category generally apply to the organization as a whole. As a result, you need to engage not only senior leadership but a diverse body of stakeholder groups like individual business units, human resources, procurement, and others. The policies in the Security category are more specifically related to your security program while the Operational category contains policies that are related to security, IT, and other areas that are responsible for managing various systems and associated controls. Finally, the Acceptable Use category applies to all users in the organization.

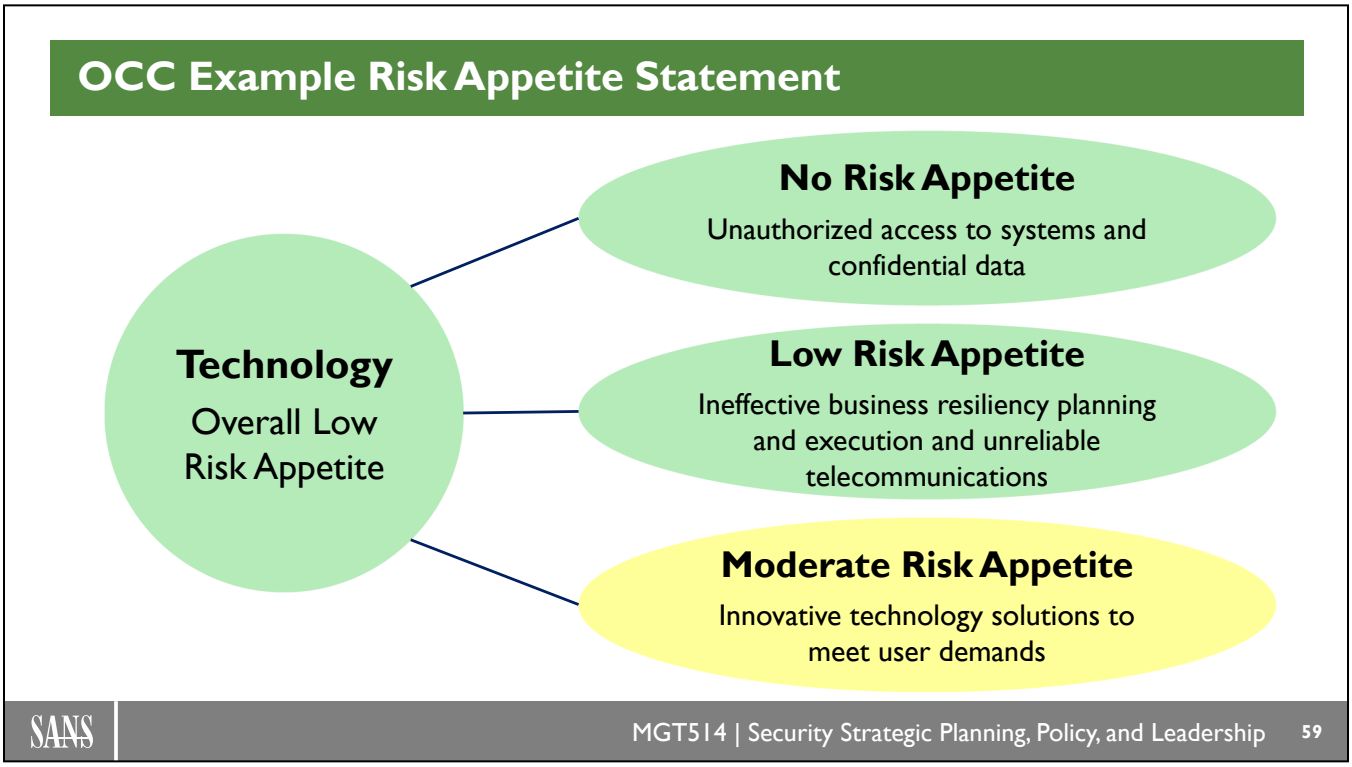
When developing or assessing policy, consider both the topics and your intended audience. In addition to the high-level policy, ensure that policy includes requirements from frameworks, compliance, and business drivers. Based on these inputs, limit policies to a specific audience. Write them so that they can be easily understood by the intended stakeholders.

Risk Appetite Statement (RAS)

- Board approved policy
  - Defines the amount and types of risk that the organization is willing to take to meet business objectives
  - Balances risk (protecting the organization) and growth (enabling the business)
- Benefits of a RAS
  - Guides and informs strategic planning and budgeting
  - Enhances understanding of risk to optimize resource allocation
  - Translates high-level strategy into more specific objectives
  - Helps build a risk-based culture



A risk appetite statement (RAS) is a critical policy that defines the amount and types of risks that the organization is willing to take to meet business objectives. This is the highest-level policy approved by the board and/or senior leadership that establishes metrics, exposure limits, and processes to ensure that risk is held within an acceptable level. This allows the organization to more clearly integrate security and risk practices into day-to-day business operations by translating high-level strategy into more specific objectives, guiding and informing strategic planning, and optimizing resource allocation. Ultimately, this helps the organization create a more risk-aware culture.



"The Office of the Comptroller of the Currency (OCC) is an independent agency entrusted with unique powers and authorities to administer the federal banking system. The OCC established its Enterprise Risk Management (ERM) function in 2015 to identify and assess OCC's mission-critical risks and support the agency in managing those risks. As part of the framework, the Risk Appetite Statement articulates the level and type of risk the agency will accept while conducting its mission."[1]

The OCC has divided their enterprise risks into nine categories: Supervision, Human Capital, Strategic, Reputation, Technology, Operational, Legal, External, and Financial. The example above shows how they have defined their technology risk appetite, which includes key security concerns. The full Technology risk appetite statement is:

"The OCC's appetite for Technology risk is low. Information systems must support core agency functions with sufficient capability, capacity, resiliency, and security from internal and external threats. The agency relies on an increasingly mobile and technologically dependent workforce to carry out its core mission. Therefore, the OCC has a low appetite for unreliable technology. The OCC will ensure a robust technological infrastructure that meets its workforce and operational needs while supporting measured innovation.

- The OCC has no appetite for unauthorized access to systems and confidential data and will maintain strong controls to mitigate external threats against its technology infrastructure.
- The OCC has a low appetite for losing continuity of business operations stemming from unreliable telecommunications or system availability. Business resiliency planning and execution must be aligned with strategic objectives.
- The OCC has a moderate appetite for innovative technology solutions to meet user demands in a rapidly changing environment. The agency will exercise appropriate governance and discipline when considering and adopting new technology."

Reference:
[1] https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/risk-appetite-statement.pdf

Risk Definitions

- Risk profile
  - Organization's overall risk at any point in time
- Risk capacity
  - Absolute maximum risk the organization can incur
- Risk appetite
  - Level of risk that the organization will accept to meet business objectives
- Risk tolerance
  - Thresholds that allocate risk appetite to certain types of risks

Since policy is key administrative control that is used to manage risk, it is important to define key risk concepts.

Risk profile:
Snapshot of the organization's overall risk at any point in time. The current level of risk for the organization.

Risk capacity:
The absolute maximum risk a company is able to incur. In certain organizations, like highly regulated financial services, organizations may have a conservative risk capacity that defines higher amounts of available capital to absorb losses. In other organizations, like startups, the risk capacity can be much higher even to the point of not being able to make payroll (at least until the next round of funding).

Risk appetite:
Overall level of risk that an organization will accept to meet business objectives. Should include both qualitative statements and quantitative metrics and limits. The risk appetite is more strategic as it helps organizations make business decisions with risk in mind.

Risk tolerance:
Thresholds that allocate risk appetite to certain types of risks, business unit, departments, etc. This can be defined as a hard or soft limit. A hard limit is when a threshold cannot be exceeded except under extreme circumstances. A soft limit is when exceeding a threshold could trigger risk review activities. The risk tolerance is more tactical as it defines limits that can be used by business units and staff to manage risk.

Risk Threshold Example

"We will continue to expand our global footprint with stores and distribution centres in locations where the exposure to [a particular weather peril e.g., flood/earthquake/bushfire etc.] will not result in business performance disruption of greater than X days over a 12 month period."

This example shows how an organization can take calculated risks to grow the business. There is a recognition that expansion can result in exposure to various natural hazards. However, a threshold is defined so that excessive risk is not incurred. As the business changes, the risk appetite can change, which may result in an adjustment to the risk threshold.

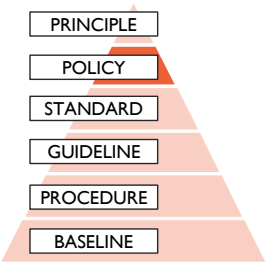
Reference:
http://www.myozone.co.uk/subsites/australia/Documents/Publications/services/BusinessRisk/W0477AU_Thought_Leadership_Article_Risk_Appetite_Statement_web.pdf

Risk Appetite Statement Example #1

Third-Party Vendor Management

We rely on business partners and third-party vendors to provide critical services. For that reason, we seek to minimize high-risk third-party vendor relationships.

Metric: High-risk third-party vendor relationships must be exited within one year, or a viable, fully tested contingency plan must be in place.



This risk appetite statement for vendor management is a high-level policy which defines that actions will be taken to minimize third-party risk. The metric is particularly important because it highlights the need to have a risk and vendor assessment program to continuously identify risk. Even more important, the organization must define tiers of risk and either mitigate the risk via a contingency plan or by finding an alternative vendor with a more acceptable risk profile.

Example from *Implementing Enterprise Risk Management: From Methods to Applications* by James Lam.[1]

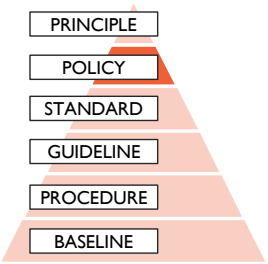
Reference:
[1] https://www.wiley.com/en-us/Implementing+Enterprise+Risk+Management%3A+From+Methods+to+Applications-p-9780471745198

Risk Appetite Statement Example #2

Cyber Risk

We manage our IT infrastructure to ensure system availability and capacity to meet business requirements as well as to protect against natural and manmade threats, including cyber attacks.

Metric: Number of IT events with material business impact will not exceed two per month. Recovery time for critical system failures will be within one hour. Automated patching program should exceed 90% of known vulnerabilities.



This is an example of another risk appetite statement for cyber risk overall. In this case, the metrics gauge the number of business-impacting events, availability, and ability to patch known vulnerabilities. Specific thresholds like these define a tolerance level and provide staff with concrete goals to target.

Example from *Implementing Enterprise Risk Management: From Methods to Applications* by James Lam.[1]

Reference:
[1] https://www.wiley.com/en-us/Implementing+Enterprise+Risk+Management%3A+From+Methods+to+Applications-p-9780471745198

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - ***Language of Policy***
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

Must and Must Not

- To be absolutely clear use "must"
  - "To impose a legal obligation, use 'must.'"[1]
  - "Use 'must' to indicate requirements. The word 'must' is the clearest way to convey to your audience that they have to do something."[2]
  - "Almost all legal writing experts agree that it's better to use 'must' to impose requirements, including contractual requirements."[3]
- To prohibit an action use "must not"
  - "Indicates a prohibition"[1]

"Must" is the only word that imposes a legal obligation and clearly indicates that something is mandatory. Numerous best practices documents state that we must use the word "must" when we want to be absolutely clear that something is a requirement.[1,2,3] Additionally, to be absolutely clear that something is prohibited, use the words "must not".

The Federal Aviation Administration (FAA) has a nice article describing the use of different words including "must".[4]

References:
[1] Federal Register Drafting Legal Documents Principles of Clear Writing, Section 3
https://www.archives.gov/federal-register/write/legal-docs/clear-writing.html
[2] Federal Plain Language Guidelines, page 25
https://www.plainlanguage.gov/media/FederalPLGuidelines.pdf
[3] FAA Writing Standards, page 4
https://www.faa.gov/documentlibrary/media/order/branding_writing/order1000_36.pdf
[4] https://www.faa.gov/about/initiatives/plain_language/articles/mandatory/

What About "Shall"?

- Do not use "shall"
  - "Imposes an obligation to act, but may be confused with prediction of future action."[1]
  - "One of those officious and obsolete words that has encumbered legal style writing for many years…outdated…imprecise. It can indicate either an obligation or a prediction."[2]
  - "Avoid using 'shall.' Shall is an ambiguous word. It can mean must, ought, or will. While shall cannot mean 'should' or 'may,' writers have used it incorrectly for those terms and it has been read that way by the courts.3[3]

Numerous best practices documents state that the word "shall" is confusing, obsolete, imprecise, and ambiguous.[1,2,3] Do not use "shall." The Federal Aviation Administration (FAA) states that "Nearly every jurisdiction has held that the word 'shall' is confusing because it can also mean 'may, will or must.' Even the Supreme Court ruled that when the word 'shall' appears in statutes, it means 'may.'"[4] They also point out that "shall" is one of the most heavily litigated words in the English language.

References:
[1] Federal Register Drafting Legal Documents Principles of Clear Writing, Section 3
https://www.archives.gov/federal-register/write/legal-docs/clear-writing.html
[2] Federal Plain Language Guidelines, page 25
https://www.plainlanguage.gov/media/FederalPLGuidelines.pdf
[3] FAA Writing Standards, page 4
https://www.faa.gov/documentlibrary/media/order/branding_writing/order1000_36.pdf
[4] https://www.faa.gov/about/initiatives/plain_language/articles/mandatory

"Should" and "May"

- When to use "should"?
  - Use for recommendations
  - "Infers obligation, but not absolute necessity"[1]
- When to use "may"?
  - Use for situations where it is up to the user
  - "Indicates discretion to act"[2]

The word "should" on the other hand is a guideline. It is not mandatory. In general, the word "should" is not recommended for policies. However, there may be some cases where you want to convey important information without making that portion of the policy mandatory. Per RFC 2119, "should" means "that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course."[3]

Some may consider "should" and "may" to be synonyms. However, they are not equivalent. The prior suggests guidance while the latter implies user choice.

References:
[1] Federal Register Drafting Legal Documents Principles of Clear Writing, Section 3
https://www.archives.gov/federal-register/write/legal-docs/clear-writing.html
[2] Ibid.
[3] https://www.ietf.org/rfc/rfc2119.txt

The Curious Case of "Will"

- Compare these two:
  - "We **must** finish tonight"
  - "We **will** finish tonight"
- Use "will" to "predict future action"[1]

You have the right to remain silent. Anything you say or do can and **will** be held against you in a court of law. You have the right to speak to an attorney. If you cannot afford an attorney, one **will** be appointed for you. Do you understand these rights as they have been read to you?

"Will" has a sense of future tense. Reserve "will" for cases where you want to indicate that something is going occur in the future.

In the United States, the Miranda warning above is a notification given by police officers to people taken into custody. It informs them that they have a right to silence but that their actions can have consequences in the future.

Reference:
[1] Federal Register Drafting Legal Documents Principles of Clear Writing, Section 3
https://www.archives.gov/federal-register/write/legal-docs/clear-writing.html

Word Choice Summary

- Guide on Drafting Legal Documents, Principles of Clear Writing

Must	Use to impose an obligation and a necessity to act
Must Not	Use to prohibit an action
Should	Use to infer obligation, but not absolute necessity
May	Use when you want to allow discretion to act
Will	Use to define future action
~~Shall~~	Do not use; may be confused with other words

The Federal Register guide for Drafting Legal Documents, Principles of Clear Writing makes it clear what certain words mean. Use "must" to create an obligation and necessity to act. Use "must not" to prohibit an action. When something is not absolutely necessary use "should". Use "may" when something is the user's choice and "will" to define actions in the future.

Finally, do not use "shall." it is ambiguous and is not a synonym for "must." It is best to avoid this word altogether.

Reference:
Federal Register Drafting Legal Documents Principles of Clear Writing, Section 3
https://www.archives.gov/federal-register/write/legal-docs/clear-writing.html

Policy and Power

- Policy is a trade-off
  - Every time we use “should” and “may,” we dilute the power of the policy
- However, very strong policies in certain situations
- As you look at examples, ask yourself:
  - Does this strengthen or weaken a policy?
  - What does the author's intent appear to be?

Policy is a trade-off. Every time we use "should" and "may," we dilute the power of the policy. However, the author of the policy may have good reasons for writing a weaker policy. Perhaps that is the only way to get something, anything approved. Or, that person might be in a situation in which very strong policies may come across as knee-jerk and not be acceptable in the culture. If people will not follow a strong policy, but they will accept a weaker, kinder, friendlier policy, that may be a win.

As you look at the numerous examples we present in the course, ask yourself:

- Does this strengthen or weaken a policy?
- What does the author's intent appear to be?

Positive and Negative Voicing

- The power of “do” and “do not”
- To define acceptable behavior
  - Use words like “must not”
- To empower people to do the right thing
  - Use words like “must do”
- When appropriate, adopt positive voicing
- Negative voice can be more effective, depending on the situation

Negative voicing, although it gets your attention, can be a turnoff. It has its place, but if overused, can turn people against the group creating and approving policy, often the security group. Try to be positive when writing policy. This can be accomplished by highlighting what employees can do. This can be empowering and help in getting people to adopt new policies instead of simply feeling constrained by restrictive policies. That being said, there is definitely a place for negative voicing. In cases where you want to be absolutely clear what should not be done include negative voicing along with positive statements.

Positive Example

Wherever possible, such sites must clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure. Users must be notified that public disclosure requests must be directed to the relevant departmental public disclosure officer.

"City of Seattle social media sites are subject to State of Washington public records laws. Any content maintained in a social media format that is related to City business, including a list of subscribers and posted communication, is a public record. The Department maintaining the site is responsible for responding completely and accurately to any public records request for public records on social media. Content related to City business shall be maintained in an accessible format and so that it can be produced in response to a request (see the City of Seattle Twitter, Facebook and CityLink standards). Wherever possible, such sites shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure. Users shall be notified that public disclosure requests must be directed to the relevant departmental public disclosure officer."[1]

Reference:
[1] http://www.seattle.gov/pan/SocialMediaPolicy.htm (Historical reference - link no longer active)

Negative Voicing: "Never"

- University of Tennessee policy example:

> When traveling with a Mobile Device, it **must never** be left unattended and unsecured
>
> Laptops **must never** be left unattended without being cable locked to a desk or table

This is the mobile device policy from the University of Tennessee. It starts with negative voicing.

Historical reference - the original link is no longer valid:
http://security.tennessee.edu/pdfs/SMDBP.pdf

Mixed Voicing

- Mixed voicing can make policy confusing to the reader:

> When traveling with a Mobile Device, it **must never** be left unattended and unsecured.
>
> Should circumstances dictate that a Mobile Device be left in a hotel room, it **must** be placed in a drawer or other location out of view of hotel cleaning staff or others who may have access to the hotel room while the user is away.
>
> Should an in-room safe of sufficient size be provided, the user **must** lock the Mobile Device inside when not in the room.

The mobile device policy from the University of Tennessee continues with a mix of positive and negative voicing. The superior statement uses the word "never," whereas some of the substatements use positive voicing. This can be confusing to the reader.

"When traveling with a Mobile Device, it must never be left unattended and unsecured.

a. Should circumstances dictate that a Mobile Device be left in a hotel room, it must be placed in a drawer or other location out of view of hotel cleaning staff or others who may have access to the hotel room while the user is away.

b. Should an in-room safe of sufficient size be provided, the user must lock the Mobile Device inside when not in the room.

c. Users must always be cognizant of the individuals around them when working on a Mobile Device in a public location. Users must exercise appropriate discretion to ensure that Confidential information cannot be seen on the screen by those around them."[1]

Reference:
[1] http://security.tennessee.edu/pdfs/SMDBP.pdf (Historical reference - link no longer active)

Mixed Voicing and Typography

Users **must not** attempt to undermine the security or the integrity of computing systems or telecommunications networks and **must not** attempt to gain unauthorized access to these resources. Users **must not** employ any computer program or device to intercept or decode passwords or similar access control information. If security breaches are observed or suspected, they **must** be immediately reported to the appropriate system administrator, departmental security coordinator, or the university information security officer.

There are a number of problems with this policy fragment. Right now, our focus is on using consistent voicing. If you do have to switch between positive and negative voicing, at least try to separate the sections into different paragraphs. A reworded example is below with positive voicing on top and additional white space:

If security breaches are observed or suspected, they must be immediately reported to the appropriate system administrator, departmental security coordinator, or the university information security officer.

Users shall not attempt to undermine the security or the integrity of computing systems or telecommunications networks and shall not attempt to gain unauthorized access to these resources. Users shall not employ any computer program or device to intercept or decode passwords or similar access control information.[1]

Reference:
[1] https://facultysenate.ucf.edu/topic/ucf-3-4-002-3-use-of-information-technologies-and-resources/

Lab 3.1: Positive Voicing

Estimated Time: 10 Minutes

- Goal of this exercise
  - Learn to translate negative into positive voicing
- There are three policy fragments in the notes
  - They all use negative voicing statements
- Look at them one at a time
  - Rewrite them using positive voicing
  - Are any of them stronger when voiced as a negative?

Changing Negative to Positive

1) Users must not undermine the security or the integrity of computing systems or networks.

2) Users must not attempt to gain unauthorized access to computing resources.

3) Users must not employ any software or device to intercept or decode passwords or similar access control information.

Lab Debrief

Note that the next slide has lab answers

This page intentionally left blank.

Voicing Summary

- People generally respond better to positive voicing
  - When you want to be absolutely clear, negative is the far better choice
  - Try not to switch between positive and negative statements
- Review your security policies to check for:
  - Word choice
  - Positive vs. negative voicing

Although we try to write policy that tells people what we want them to do, sometimes it is a lot shorter and to the point to say something in the negative. The most important point is to try not to flip-flop between the two. If you can put your positives in one list and your negatives in another, you can have the best of both worlds.

Here are examples of how you can turn negatively voiced statements into positively voiced statements:

Negative #1: “Users must not undermine the security or the integrity of computing systems or networks.”
Positive #1: “Users must use computing resources and networks for their intended purposes.”

Negative #2: “Users must not attempt to gain unauthorized access to computing resources."
Positive #2: “Authorized use is permitted.”

Negative #3: “Users must not employ any software or device to intercept or decode passwords or similar access control information.”
Positive #3: “Users must respect access control requirements.”

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - ***Policy Structure***
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

One or Many?

- Large, monolithic policy document
  - Sixty-page security policy
  - Hard to update
- Short security policy document
  - Six-page security policy
  - Hard to be comprehensive
- Many 1.5-page policies as needed
  - May be most ideal

There are many decisions to make when doing policy. One is the format. Some organizations prefer a single 50- to 60-page security policy. The problem with this is that it is hard to update. People don't want to read a 50-page email attachment, so they put off the review.

A growing number of organizations want to condense security into a 5- or 6-page security policy. The problem with this is that it is hard to be comprehensive, and you have to ignore a number of use cases.

Using as many 1.5-page policies as needed may be most ideal, but they have to be managed.

Reference:
http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf

Components of a Policy Document

- Overview or background
- Purpose
- Scope
- Policy statement
- History
  - Publication date
  - Cancellation or expiration date
  - Version history
- Enforcement
  - Penalties for policy violations
- Responsible parties
  - Roles and responsibilities
- Related documents
  - Other relevant policies
  - References to compliance standards
  - Glossary and definitions

- Purpose or Overview: Security policy usually contains a statement, often at the beginning, describing the reason the policy is being established and any associated goals.
- Related Documents: These are often titled "References" and usually cite higher-level policy or implementation guidance.
- Cancellation: A new or updated policy may supersede an existing (perhaps outdated) policy. This section identifies those policies and clarifies what is actually in effect.
- Background: This optional section provides information amplifying the need for the policy. It may also provide historical information relevant to the subject.
- Scope: This section identifies the depth and breadth of coverage (to whom or what the policy applies). Is it for one element of the organization, or will it also apply to contractor agencies who work for your organization?
- Policy Statement: This statement identifies the actual guiding principles or what is to be done. These statements are designed to influence and determine decisions and actions within the scope of coverage. The statements should define actions that are prudent, expedient, or advantageous to the organization.
- Responsible Parties: The security policy document states who is responsible for what. Typical positions that might be addressed include the head of the corporation, the CIO, people in the Legal department or in Human Resources, system administrators, and information security officers. Subsections might identify how additional detailed guidance will be developed and provided, plus the frequency of policy review. Methods or techniques for measuring compliance may also be included in this section (in addition to identifying parties responsible for the audit).
- Action: This section specifies what actions are necessary and when they are to be accomplished. It may identify the time frame in which additional guidance (mentioned above) will be forthcoming. Hopefully, the policy meets the criteria stated above, but there may be a need for a waiver process. This is one logical place to identify that process and the time frame for completion and who should conduct the policy review.

Note that not all sections are required. If your search for a Policy Development Guide was successful, consult it to determine required sections. If there is no written guide, use the preceding template and check with other folks who have been successful in getting other policy signed and implemented.

Purpose Fragments: Examples

"Improved recovery times"

"Reduced costs or downtime due to loss of data"

"Reduction in errors for both system changes and operational activities"

"Regulatory compliance"

"Management of confidentiality, integrity, and availability"

The Purpose defines why a policy is necessary. This can include items such as regulatory constraints, data protection, improved recovery times, or reduction in errors.

Purpose Example: Access Control

Human threats are the primary cause for a wide range of hazards to business systems and information.

Unauthorized users could obtain and misuse confidential info.

Authorized users could fail to follow system instructions and properly protect data.

To mitigate human threats, the organization will establish access controls that limit access to sensitive systems and information to the minimum necessary level to support organizational service delivery.

This is a sample Purpose statement for an access control policy. It acknowledges that human threats can be the source of a wide variety of security issues. There is an understanding that these issues may be caused by malicious or negligent actors. To mitigate these threats, access must be limited to the minimum level necessary to provide service.

Scope Example: Brown University

This policy applies to all users of computing resources owned or managed by Brown University. Individuals covered by the policy include (but are not limited to) Brown faculty and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals and organizations accessing network services via Brown's computing facilities.

This policy goes on to say: "Computing resources include all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network."[1]

Reference:
[1] http://www.brown.edu/information-technology/computing-policies/acceptable-use-policy

Document History

- Current version information
  - Publication/effective date
  - Version number
- Version history
  - Change summary per version
  - Version numbers and dates
- Cancellation/expiration date
  - Force a review by adopting a life-cycle approach
  - Global policy defines review period (for example, every 1–2 years)

There is a tendency to "fire and forget" when it comes to policy. This is not ideal. It is far wiser to adopt a life-cycle approach to policy. One of the keys to making it work is assigning an expiration date to the policy as part of the approval process. The expiration date triggers a review. If the policy is not reviewed, it becomes void.

The review can often be done at a far lower level than the approval. There are a couple of questions to ask during the review:

- Is there still a risk?
- Is the enforcement section of the policy effective?
- Is the policy still needed?

If the answer to these three questions is yes, generally someone like the CISO can approve the policy. Now, the next question is this:

- Does the policy need to be updated?

If the policy needs to be changed substantially, it probably needs to go back through the review process.

Policy Enforcement

- Typical penalty or sanction defined in policy
  - "Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment"
- Is this a reasonable penalty for
  - Clean desk policy violations?
  - Some personal internet use?
- Penalties should be even-handed
  - Often enforced by HR

A standard penalty for failing to comply with policy is usually stated like this: "Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment."

Such a statement is typically included to ensure that the employer has the most latitude in determining the appropriate punishment for a violation. However, it is best to define reasonable punishments that, although not being excessive, still work to shape appropriate behavior. For example, in some environments, termination may not be appropriate for a violation of the clean desk or internet-use policies. However, it may be absolutely appropriate in highly secure environments.

What is an appropriate level of enforcement? Ideally, this is the same for all policies, security or otherwise. In many cases, it is the responsibility of the line manager, but then you run into uneven enforcement. One manager might give a person a day off without pay, whereas another gives an employee a "talking to" for the same infraction. Human Resources (HR) is typically the most appropriate enforcement entity.

Grocery Store Example

- John Schultz observed a customer shoplifting
  - Attempted to stop shoplifter after he left store
  - Terminated for violating Whole Foods policy against "touching customers”
  - Many people were angry with Whole Foods
- Grocery store manager Ray Augusta caught stealing
  - Identified by security cameras and loss prevention officer
  - He was terminated and sued the employer
  - Rules must be distributed, known by employees, clear and understandable, consistently enforced
  - Employees must be warned that a violation could result in termination

"John Schultz, the Whole Foods Market employee who was fired after he tried to stop a shoplifter, said he has received several job offers and lots of support from the public after publicity over the incident. Kate Klotz, a spokeswoman for Whole Foods Market, said Thursday in a statement that the safety of employees, customers, and the community comes first.

'Please consider the potential consequences if the suspected shoplifter had a gun or knife or if the team member had caused an accident while crossing a five-lane road in pursuit of a shoplifter,' she said. 'Groceries can be replaced, but human life cannot.' Security systems and trained personnel are in place in stores to handle shoplifters, she said. Company policy, she said, restricts employees from physically confronting others.”

In another case, a grocery store manager was caught stealing. He was terminated but sued. The case highlighted that a policy must be distributed, known by employees, clear and understandable, and consistently enforced. Moreover, employees must be warned of the consequences.

References:
https://www.mlive.com/annarbornews/2008/01/fired_whole_foods_worker_gets.html
http://www.retailwire.com/discussion/12655/whole-foods-fires-worker-for-stopping-shoplifter
https://toronto-employmentlawyer.com/breach-company-policy/

Responsible Parties

- Roles and responsibilities must be defined
- Who does what?
  - Information Security
  - Information Technology (IT)
  - HR, Legal, Compliance
  - Internal Audit
  - Business Units
  - Different departments

Policies should define who is responsible for executing and enforcing the items defined in the policy statements. Often, organizations that do not define overall responsibility can find it difficult to actually execute on the tasks at hand. This can cause confusion between areas like IT and Information Security that often have to work closely together. Additionally, responsibility for assessing, monitoring, and auditing various controls should be assigned to certain groups like Information Security or Internal Audit. Ideally, various business units will also have some responsibility for contributing to the security posture of the overall organization.

Related Documents

- Provide references to other documents
  - Powerful way to manage policy and procedure
- Include items such as
  - Standards references
  - Compliance requirements
  - Other policies and procedures
- Online policy library
  - Easy way to reference other documents
  - Track when people have viewed documents

Example References

CIS Critical Controls
CSC #3, 8, 10

NIST 800-53
SC-8, SC-9, SC-12

ISO 27000
10.8, 10.9

PCI DSS
Requirement 7

HIPAA
164.310 (d)(1)

Wikipedia is the largest encyclopedia in the world. If you look at a Wikipedia page, it is very common for it to link to other Wikipedia pages. This is an excellent model for policies and procedures. They can link to one another to make them easy to find. Another advantage to using your intranet website to publish your policies and procedures is that when you announce a new policy, you can use your weblogs to see who did or did not click on it. You can't usually tell if the employees read it, but you can see if they opened it. If you have 1,000 employees and only 10 open the policy, that tells you something about the effectiveness of your program.

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - ***Policy and Culture***
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

Organizational Assumptions, Beliefs, and Values (ABVs)

- Assumption
  - Premise that is taken for granted
  - Difficult to change
- Belief
  - State in which a proposition or premise is held to be true
- Value
  - Ideal accepted by an individual or group
  - "He has old-fashioned values"

"Organizational cultures, like other human cultures, include particular types of artifacts, special values, and common beliefs and assumptions. In some respects, it is the culture that makes the organization a true organization rather than just a collection of randomly engaged people. It provides the defining characteristics that make organizations differ from each other, and the foundation for both success and failure organizationally. While organizational culture is, to some extent, organic, it is somewhat malleable, and management needs to focus on those aspects of the culture which can be influenced and shaped."

"Organizational culture is the sum of values and rituals which serve as 'glue' to integrate the members of the organization." – Richard Perrin

References:
http://www.lotsofessays.com/viewpaper/1691941.html
http://blogs.hbr.org/2013/05/what-is-organizational-culture/

ABV Example

- Internet Acceptable Use policy at a university
  - How in tune with the university culture is this policy?
  - What will the faculty reaction be?

> Except in isolated or occasional circumstances, the computing and telecommunications resources of the university shall be used only for purposes directly related to or in support of the academic, research, or administrative activities of the university. If a university employee wishes to use university facilities, students, equipment, materials, or software for personal or outside professional purposes, permission must be obtained in advance using form AA22 (faculty members) or HR-12 (A&P or USPS).

This policy does not fit the open culture of many universities. Faculty and staff have

1) An assumption that computing resources will be readily available
2) A belief that access to data and knowledge is a personal right
3) Values of education, research, openness, and collaboration

Restricting computing use to "only purposes directly related to or in support of academic, research, or administrative activities of the university" and requiring bureaucratic processes to obtain permission for personal use is in direct contradiction to the assumptions, beliefs, and values of the higher education community.

Reference:
https://policies.ucf.edu/documents/4-002.pdf

Security Culture

- Have you ever read a policy so ridiculous you knew you would never follow it?
- Policy must be congruent with the culture of the organization
- We meet the organization where it is and make changes slowly

"It is not necessary to change.
Survival is not mandatory."

- W. Edwards Deming

"Things do not change; we change." – Henry David Thoreau

Our policy cannot be outside of the cultural norms of our organization, or it will not be followed. This would also impact the effectiveness of all other policy. We meet the organization where it is and make change slowly; change is difficult for people and organizations.

"Changing culture in many ways parallels farming. The first phase, Analysis and Objective Setting, is dedicated to analyzing and preparing the soil. Phase II, Systems Introduction, plants the seed of change. The third phase, Systems Integration, is the cultural equivalent of adding fertilizer and water so that the plant takes root and flourishes. And the fourth phase, Evaluation, Renewal, and Extension, is similar to harvesting the crop and gathering new seed for the next planting."

Reference:
http://www.new-paradigm.co.uk/Culture.htm

Organizational Culture

- To develop or assess policy accurately
  - Must understand the overall culture of the organization
- Culture is exhibited in a number of ways:
  - Formal versus casual
  - Dress code
  - Drug testing
  - Dating within the organization
  - Time clock enforcement
  - Team versus individual effort
  - Freedom to work from home
  - Creativity is encouraged or discouraged
  - Jobs versus careers
  - Commitment to ethics, law, morals

We have to understand an organization's culture to write policy that fits. Here is a description of Organizational Culture from managementhelp.org:

"Basically, organizational culture is the personality of the organization. Culture is comprised of the assumptions, values, norms and tangible signs (artifacts) of organization members and their behaviors. Members of an organization soon come to sense the particular culture of an organization. Culture is one of those terms that's difficult to express distinctly, but everyone knows it when they sense it. For example, the culture of a large, for-profit corporation is quite different than that of a hospital, which is quite different than that of a university. You can tell the culture of an organization by looking at the arrangement of furniture, what they brag about, what members wear, and so on—similar to what you can use to get a feeling about someone's personality.

"Corporate culture can be looked at as a system. Inputs include feedback from, e.g., society, professions, laws, stories, heroes, values on competition or service, etc. The process is based on our assumptions, values and norms, e.g., our values on money, time, facilities, space, and people. Outputs or effects of our culture are, e.g., organizational behaviors, technologies, strategies, image, products, services, appearance, etc.

"The concept of culture is particularly important when attempting to manage organization-wide change. Practitioners are coming to realize that, despite the best-laid plans, organizational change must include not only changing structures and processes, but also changing the corporate culture as well."

Reference:
https://managementhelp.org/organizations/culture.htm

Security Culture Tip-offs

- Network/web traffic is monitored
  - Access to sexually explicit sites
- Desktop lockdown
  - Users cannot install or download software
- Physical security
  - Subject to physical search, strict limitations on allowed devices
- Trust for all connections initiated inside organization
  - No egress filtering
- Configuration management
  - Users cannot change settings

The pragmatic next step in developing the framework is to assess the security posture, the amount of progress an organization has made toward implementing a culture of security. The mission statement of an IT-focused company is very helpful; in fact, some companies even have security mission statements! Let's consider the mission statement of SecureAddress:

"It is the policy of SecureAddress.com to provide the most secure environment possible for our customers."

It wouldn't take long to determine if the company is living up to that! More likely, you will be assessing whether there is a culture of security—that is, the degree to which security is part of business operations. Understanding the true security posture helps you evaluate policy to see whether it has the correct tone for your site.

The following is a good start as a checklist to help you assess the posture of an organization:

- Wander around the organization without a badge to see if anyone challenges you.
- Call someone to see if he or she is willing to send you documents that have not been approved for public release.
- Run a password assessment tool. If half the passwords are named after the user's favorite sports team, that's a bad sign. (Make sure you have written permission to do this!)

A few simple questions can help determine the level of security controls at a site. Some to ask follow:

- Evaluate the commitment of senior management to physical, information, and intellectual property security. At the same time, evaluate the level of risk senior management is willing to accept. If there is no commitment from senior management, there cannot be a culture of security.
- Evaluate the presumption of privacy, including phone and network monitoring. Do employees have a reasonable expectation that the files on their computers and their phone and internet communications are protected?

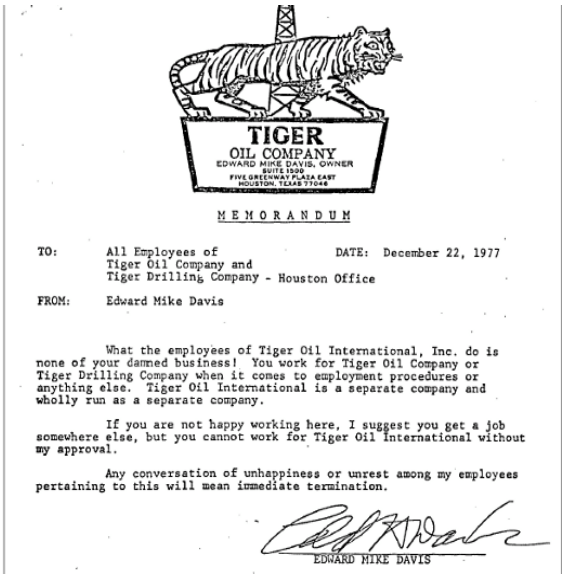
- Does company policy allow random physical searches, and is there an active search program?
- Is the perimeter configured to allow all connections initiated inside the organization?
- What is the level of employee awareness of security practice? Do employees know procedures for developing and protecting information systems? Is the employee able to add software or modify settings on the desktop system?
- Are administrators able to make changes without going through a formal configuration-management approval program?
- Can the internal auditors name a dozen technical security protective or detective controls without looking for them?

Additional points to consider are as follows:

- Formal versus casual dress code
- Drug testing
- Dating within the organization
- Time clock enforcement
- Freedom to work from home
- Team versus individual effort
- Whether creativity is encouraged or discouraged
- Jobs versus careers
- Commitment to ethics, law, culture, morals

The types of questions we list here help us to define the importance and degree of implementation of security. They help us understand where the organization is in their journey toward a culture of security. Knowing this will be necessary as we try to establish a baseline to be able to evaluate policy.

Coercive Management Style



TIGER
OIL COMPANY
EDWARD MIKE DAVIS, OWNER
SUITE 1500
FIVE GREENWAY PLAZA EAST
HOUSTON, TEXAS 77046

MEMORANDUM

TO: All Employees of Tiger Oil Company and Tiger Drilling Company - Houston Office

DATE: December 22, 1977

FROM: Edward Mike Davis

What the employees of Tiger Oil International, Inc. do is none of your damned business! You work for Tiger Oil Company or Tiger Drilling Company when it comes to employment procedures or anything else. Tiger Oil International is a separate company and wholly run as a separate company.

If you are not happy working here, I suggest you get a job somewhere else, but you cannot work for Tiger Oil International without my approval.

Any conversation of unhappiness or unrest among my employees pertaining to this will mean immediate termination.

EDWARD MIKE DAVIS

Part of your checklist is to identify the management style of your organization. Look at both the top of the organization and whomever you are reporting to or whoever has hired you as a consultant to determine if management is autocratic (e.g., leader makes all decisions unilaterally) or permissive (e.g., leader permits subordinates to take part in decision making and also gives them a considerable degree of autonomy in completing routine work activities).

The memorandums from the Tiger Oil Company are an amazing look into the culture created by CEO Edward Mike Davis. In 1980, Tiger Oil Company filed for bankruptcy. Other letters from Edward Mike Davis of Tiger Oil Company can be found at http://www.lettersofnote.com/2010/08/tiger-oil-memos.html

The letter is transcribed below so it is easier to read.

DATE: December 22, 1977
TO: All Employees of Tiger Oil Company and Tiger Drilling Company - Houston Office
FROM: Edward Mike Davis

What the employees of Tiger Oil International, Inc. do is none of your damned business! You work for Tiger Oil Company or Tiger Drilling Company when it comes to employment procedures or anything else. Tiger Oil International is a separate company and wholly run as a separate company.

If you are not happy working here, I suggest you get a job somewhere else, but you cannot work for Tiger Oil International without my approval.

Any conversation of unhappiness or unrest among my employees pertaining to this will mean immediate termination.

What Would the Approach to Policy Be If…

- Management style was collaborative?
- Management style was charismatic
  - Example: Steve Jobs at Apple?
- Management style was top-down or authoritarian
  - Example: Military?

If the management style is collaborative, you would want to make extensive use of a policy steering committee, having representation from as many parts of the organization as possible.

If the management style is consultative, you would want to find someone with "referent power," a person everyone likes and trusts, and make sure he or she is on your steering committee.

If the management style is charismatic (such as Steve Jobs at Apple), you would want to find someone the leader trusts to do the detailed operations work and have that person on the policy steering committee if possible, or if not, someone that person trusts.

If the management style is top-down or authoritarian, such as most of the DoD, there would be a fixed process for policy development and approval. You are not going to be able to change it or ram a policy through—at least not often. So, think ahead and get the drafts going.

If the management style is coercive, this gets tough. The best answer is to work on your job skills and resume. However, in the meantime, never rise to argument. Ignore the parts of an email that are mean or inflammatory. When replying to such an email, delete everything in your response except for items pertaining to the matter at hand.

Distorted Perceptions

- Culture can be positive or negative
- Microsoft example:
  - Belief that there should be "A computer on every desk and in every home, running Microsoft software"
  - Success created an assumption that Windows should run everywhere
  - Tried to continue to leverage dominance of Windows and Office on mobile

"What makes companies great is inevitably what makes companies fail, whenever that day comes."

- Ben Thompson

We need to be sensitive to the way people and, in fact, whole organizations filter information. If the majority of people are thinking tactically, then policies that address long-term strategy will probably not be effective. Hubris is a tough one. If the organization was formerly great and has been catastrophically downsized, people are very open to change. However, if the organization is on a slow decline, people tend to be proud and resistant to change. One of the great examples of urban myth reinforcement is a hospital emergency room. Despite all statistics to the contrary, if there is a full moon, they believe more accidents are going to happen.

Every organization develops a core set of assumptions, beliefs, and values that become rules that govern behavior in the workplace. Corporate culture is a system of shared values, assumptions, beliefs, and norms that unite the members of an organization. Corporate culture aligns employee behavior, develops organizational commitment, and provides social workplace guidelines. However, what happens if it goes too far astray from reality? Some potential pitfalls are:

Nearsightedness: Totally tactical, no strategic thinking
Hubris: So sure that you will always be dominant
Denial/Defensive Behavior: "Everybody hates us; we are going to be weird"
Urban Myth Reinforcement: Everybody who has ever worked in an emergency room "knows" that on a full moon . . .
Groupthink: We hire people exactly like ourselves

Ben Thompson, in his article The Curse of Culture, describes the case of Microsoft. Its great success dominating the PC landscape led to an assumption that Windows should run everywhere. As the mobile boom was occurring, former CEO Steve Ballmer famously laughed at the iPhone and continued to push a "One Microsoft" strategy focused on Windows. What was a strength? The focus on Windows, that generated billions in profits, had resulted in hubris and an inability to react appropriately to the new computing landscape.

Reference:
https://stratechery.com/2016/the-curse-of-culture/

Culture and Exception Requests

- Policy exception requests may
  - Stem from special causes
  - Mean that the policy is technically incorrect
  - Indicate that policy does not fit into the culture
- Sudden spike in exception requests
  - Reveal that something has changed
  - Try to predict and identify drivers of new behavior

As security managers, we want to keep an eye on requests for exceptions to a policy. This is often down at a fairly low level in the organization, and there is a risk that the information will not be reported up to the security manager. One key to being effective, to having situational awareness, is to place yourself in the information stream. Consider using technology to have copies of exception requests sent to your inbox. Coach the person granting exceptions to study the root cause. Is it a special cause, a very rare event such as a thousand-year flood, or a common cause, something that is likely to happen again?

It All Comes Down to a Simple Question

- From a security perspective
  - How liberal or conservative is your organization?
- You can have too much policy
  - Create policy that maps to your security maturity
  - Don't codify something into policy that your organization is not yet ready to accomplish

The needs assessment comes down to one rich question, "Where is your organization against a security maturity scale?" Along the way, you probably learned some significant risk areas that you want to address with policy. Rank them by risk in a way that will be acceptable to your organization's culture. Begin to make change one step at a time.

This page intentionally left blank.

CYBER42

Event #8

Debrief

This page intentionally left blank.

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - ***Define Requirements***
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

Gather Data

- Identify requirements by gathering organizational data
  - Interviews
  - Industry trends (for example, PEST)
  - Gap analysis (for example, SWOT)
  - Audit findings
  - Review of security program and activities

Requirements for security policies can be identified using data gathering techniques such as:

- Interviews with all key groups and organizations identified.
- Conversations and interviews with management, owners of general support systems and major applications, and other organizational staff whose business functions rely on IT.
- Organizational surveys.
- Review and assessment of available resource material, such as current awareness and training material, training schedules, and lists of attendees.
- Analysis of metrics related to awareness and training (for example, percentage of users completing required awareness session or exposure, percentage of users with significant security responsibilities who have been trained in role-specific material).
- Review of security plans for general support systems and major applications to identify system and application owners and appointed security representatives.
- Review of system inventory and application user ID databases to determine all who have access.
- Review of any findings and/or recommendations from oversight bodies (for example, Congressional inquiry, inspector general, internal review/audit, and internal controls program) or program reviews regarding the IT security program.
- Analysis of events (such as denial of service attacks, website defacements, hijacking of systems used in subsequent attacks, successful virus attacks) that might indicate the need for training (or additional training) of specific groups of people.
- Review when technical or infrastructure changes are made.
- The study of trends first identified in industry, academic, or government publications or by training/education organizations. The use of these "early warning systems" can provide insight into an issue within the organization that has yet to be seen as a problem.

Documentation Baseline

- Review existing documentation
  - Policy, Standard, Guideline, Procedure, Baseline
- Ensure that there is a high-level policy
  - Senior-level commitment for information security
  - Typically, an overarching Information Security Program Policy or letter of endorsement
- Identify unstated rules
  - Management directives that affect the organization

A baseline is our foundation for evaluating policy, and it is made up of several components. We have the mission statement that defines what customers, suppliers, and employees should be able to expect from the organization. We have the assessment of the organization's security posture, which is a bit like looking in a mirror; our mission statement is the way we hope people view us; our security posture is what we actually look like. Now we can begin to evaluate what policies we are missing. As you know, policy exists on several levels. Hopefully, everything is organized and up-to-date. If not, you need to begin the search for written guidance.

Enterprise-wide or corporate policy is the highest level of policy and consists of a high-level document that provides a direction or thrust to be implemented at lower levels in the enterprise. This is typically a high-level policy or a letter of endorsement from senior management. This policy must exist to properly assess lower-level policy. If this policy does not exist, begin work to create this policy document and get it approved before attempting to assess lower-level policy. This enterprise- or corporate-level security policy is the demonstration of management's intent and commitment for the information security in the organization. This should be based on facts about the criticality of information for business as identified during our assessment and evaluation of security posture. A security policy statement should strongly reflect the management's belief that if information is not secure, the business will suffer. The policy should clearly address issues like these:

- Why is information strategically important for the organization?
- What are business and legal requirements for information security for the organization?
- What are the organization's contractual obligations toward security of the information pertaining to business processes, information collected from clients, employees, and so on?
- What steps will the organization take to ensure information security?

A clear security policy will provide direction to the information security efforts of the organization and create confidence in the minds of various stakeholders.

The chief executive of the organization should issue or act as the approving authority of the security policy statement to build the momentum toward information security and set clear security goals and objectives.

Identify Problem or Risk

- Policy requirements can come from
  - Unexpected events
  - Anomalous issues
  - Security incidents
- Requirements ideally identified via regular processes such as
  - Vulnerability assessments
  - Penetration tests
  - Tabletop exercises

Ideally, requirements for security policies would be identified via regular processes that we have instituted as part of the security program, such as vulnerability assessments, penetration tests, and tabletop exercises. In reality, however, new risks are usually identified as a result of unexpected events. An anomalous issue might be detected, resulting in new action that is necessary. A security incident highlights previously unknown problems and weaknesses. In response to these issues, we must update or create corresponding security policy.

Policy Planning

- Policy development requires
  - Planning to address potential risks
  - Understanding of organizational culture
  - Socialization with key stakeholders
- Conduct tabletop exercises
  - Determine how your organization will interact with requests from law enforcement
  - Make contact with local, state, and federal law enforcement officials before needing their services

Policy planning is important because it helps you determine what steps need to be taken *before* an event occurs. It is important to conduct tabletop exercises and/or cyber simulations. Specifically, consider conducting ransomware tabletop exercises that engage all levels of the organization so you can prepare for how to deal with a similar situation in your business. Part of this planning also includes exchanging contact information and developing relationships with local, state, and federal law enforcement officials. You should also determine how your organization wants to interact with requests from law enforcement by identifying the impact to the business based on various decisions that could be made.

Risk Analysis

- In security, we focus on risk
  - How bad could it be?
  - How likely is it to happen?
- Policy is a key administrative control
  - Used to manage risk
  - Can often be more effective and less expensive to write policy
    - Compared to implementing a new technology control

Risk management is the same in many fields. It is the mathematical probability that a threat will cross a matching vulnerability. The practical approach is to ask two questions:

- How bad could it be?
- How likely is it to happen?

Often, we focus on countermeasures to reduce the likelihood. One of the key administrative controls we have at our disposal is to create policy that can help manage the risk. Creating new policy can often be less costly than purchasing and implementing a new technology control. This can be true even after factoring in the cost of policy awareness, training, and enforcement.

Consider All Use Cases

- Developing good policy requires
  - Analysis of all use cases
- Incorporating various use cases into policy
  - Reduces exception requests
  - Streamlines policy enforcement process
  - Minimizes bottlenecks from the security team

One of the keys to writing good policy is to think through all the possible use cases. Because there are a number of possibilities in any given situation, we may need to reword policy or explicitly define various exception cases that may not be obvious initially. By incorporating additional use cases into policy, we can reduce exception requests, streamline the policy enforcement process, and minimize bottlenecks created by delayed security team review of various exception requests.

Example #1: Illegal Drugs

- Drugs are forbidden except…

> The possession, use, manufacture, or distribution of any controlled substances or paraphernalia on University property is strictly prohibited.
>
> Any person found in possession of a controlled substance or drug paraphernalia will be turned over to the appropriate law enforcement agency for criminal prosecution.
>
> **The exception to this policy is authorized law enforcement officers or other approved personnel, for the purposes of lecture, training, or demonstration.**

Your organization may have a strict "no drugs" policy. However, in considering all use cases, it is important to clearly define exceptions. The example on the slide highlights a common scenario where law enforcement may be required to utilize controlled substances "for the purposes of lecture, training, or demonstration.

Reference:
http://www.yk.psu.edu/Information/Safety/regulations.htm (link no longer active)

Example #2: Weapons and Firearms

- Weapons are forbidden except…

> It is a violation of policy for any person to possess, carry, or use any weapon, ammunition, or explosive on University owned or controlled property. Any person found in violation of this policy is subject to criminal prosecution and/or University discipline.
>
> **The only exception to this policy is authorized law enforcement officers or other persons specifically approved by the University.**

The policy fragment above clearly defines exceptions for both law enforcement officers and "other persons specifically approved by the University." In this case, the policy writers likely know about certain special circumstances that arise where other individuals are required to carry firearms. Including this provision in the policy helps eliminate confusion and unnecessary exception requests that may arise. The specific details of the types of individuals that may need approval can be described in more detailed guidelines or procedures.

Reference:
http://www.yk.psu.edu/Information/Safety/regulations.htm (link no longer active)

Example #3: Animals in Office

- Animals are forbidden except…

> Pets are not permitted inside campus buildings.
>
> **This rule shall not apply to seeing eye dogs, authorized animal research or training conducted on Penn State property, and dogs being used by law enforcement agencies.**

This policy fragment defines exceptions to the policy regarding animals and pets on premises. A thorough understanding of personal requirements (for example, seeing eye dogs), business practices (for example, animal research or training), and legal requirements (for example, dogs being used by law enforcement) help us create policy that is practical, enforceable, and more likely to be adopted.

Reference:
http://www.yk.psu.edu/Information/Safety/regulations.htm (link no longer active)

Levels of Policy

- There can be multiple levels of policy:
  - Regulation and law
  - Enterprise-wide/corporate/governing policy
  - Division-wide policy
  - Local policy
  - Issue-specific policy
  - System-specific policy
  - Procedures

A policy can exist on different levels within an organization. Unless you are at the top of the organizational hierarchy, it is likely that a part of the organization above your level issues policy you are expected to implement. A common hierarchy for policy in an organization looks like this:

- **Enterprise-wide, Corporate, or Governing Policy**: This policy consists of documents from the highest level (perhaps national or worldwide) within the organization that provide a general direction to be implemented at lower levels in the enterprise.
- **Division-wide Policy**: This policy consists, typically, of an amplification of enterprise-wide policy and implementation guidance. This level might apply to a particular region of a national or multinational organization.
- **Local Policy**: This policy contains information specific to the local organization or corporate element. May also be site specific.
- **Program Policies**: This high-level policy sets the overall tone of an organization's security approach. Typically, this policy provides guidance to enact the other types of policies and defines who is responsible. This policy can provide direction for compliance with industry standards, such as International Standards Organization (ISO), the British Standards Institute (BSI), the Institute of Electrical and Electronic Engineers (IEEE), and the National Institute of Standards and Technology (NIST), as well as with applicable business and government regulations.
- **Issue-specific Policy**: These are intended to address specific needs within an organization including password procedures, internet usage guidelines, antivirus, and so on. This is not as broad a category as the program policy; however, it is broader than system-specific policy.
- **System-specific Policies**: These might be necessary if your organization has different systems performing different functions. The use of one policy governing all of them might not be appropriate. It might be necessary to develop a policy directed toward each system individually. For instance, a systems policy might specify a much more rigorous set of procedures for a system that is accessible from the internet, such as a DNS server, than a protected desktop system.
- **Security Procedures and Checklists:** These consist of local standard operating procedures (SOPs), aligned with and perhaps derived from security policy.

Security policy might exist on some levels and not on others. Documents interact and support one another and generally contain many of the same elements. In a typical organization, policy written to implement higher-level directives may not waive any of the requirements or conditions stipulated at a higher level. Security policy must always be in accordance with local, state, and federal computer crime laws, in addition to other applicable government statutes.

Policy Hierarchy:
The first step in policy assessment is to ensure you understand where the policy fits in the hierarchy. The reason is that higher-level policies will be more general and tend to have sweeping statements, and lower-level policies are much more specific.

Security policy might exist on some levels and not on others. You might not need a division-wide policy for every division. Documents interact and support one another and generally contain many of the same elements. This is almost always true in a multinational organization. For example, the legal framework is different in France, Australia, and the United States. This could have a profound impact on the specifics of policy. However, the policy attempts to achieve the same effect in all three countries, so the similarities probably exceed the differences. In a typical organization, policy written to implement high-level directives does not relieve (waive) any of the requirements or conditions stipulated by high-level policies. After all, we really can't have the data center manager overturning policy signed by the Chief Executive Officer of the company. In addition, security policy must always be in accordance with local, state, and federal computer-crime laws and regulations.

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - ***Development Examples***
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

Development Examples

- Acceptable Use
  - Email
  - Mobile
- Secure Development

This page intentionally left blank.

Email Risks

- Data loss
  - Email forwarding to noncorporate account
  - Sending sensitive documents
  - Proprietary and confidential communications disclosed
- Fraudulent activity
  - Spam, phishing, spear phishing
  - Business email compromise
- Improper use
  - Inappropriate use of "all employees" list
  - Defamation, comment spam

For email, we again start by identifying a need or a risk that requires us to update or create policy. Email risks include data loss, fraudulent activity, and improper use that can be caused by a variety of actions such as maliciously or negligently forwarding sensitive documents, phishing/spear phishing, and general inappropriate use.

One-Sentence Position Statement

Though email is often considered informal, messages are actually official corporate communications and must be carefully considered before being sent.

The purpose of a policy can be best represented by the one-sentence position statement. Email can often be utilized as an informal communication mechanism, but the recipient of an email can construe it as an official corporate communication. As a result, it's important to carefully consider the message before sending.

Positive Voicing Examples

Individual electronic mail accounts are issued solely for the use of the individual to whom they have been assigned.

Use good judgment when opening or forwarding email. Email from an unknown location with an attachment must be opened with care or deleted. Some email may contain viruses or programs used to attack our systems.

In trying to address the risk of infection via spam phishing, it would be easy to have a policy statement stating, "Do not open unknown attachments." However, that statement would be unrealistic. How would a user know whether or not an attachment can be trusted? The policy fragment above takes a more measured approach by stating that attachments must be opened with care.

This fragment also addresses inappropriate sharing of email account access.

Both of these fragments are worded in a positive voice, which makes the policy much friendlier.

Negative Voicing Examples

Email users **must not** knowingly:

Send credit card data or personally identifiable information (PII) via unencrypted email.

Send offensive or disruptive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Forward proprietary corporate email to personal email accounts.

This policy fragment uses negative voicing. For policies like Acceptable Use, it is often useful to have both "acceptable" and "unacceptable" use sections within the policy document. That way, readers can more clearly understand what is and what is not allowed.

Security Controls

- Ensure that policy defines requirements that can be implemented
- Two primary types of email controls
  - Technical
    - Data Loss Prevention (DLP)
    - Spam filtering, Anti-malware
    - Encryption, Email signing
    - Restricting access, multifactor authentication
    - Secure email portal
  - Administrative
    - Awareness and education
    - Phishing campaigns

As the policy is created, it is important to determine how the policy requirements can actually be implemented. For email, a variety of technical and administrative controls could be utilized:

- **Data Loss Prevention (DLP):** Identifying sensitive data being sent out of the organization
- **Spam Filtering/Anti-malware:** Preventing malicious documents from being sent to employees
- **Encryption/Email Signing:** Ensuring that data is protected, and the sender is authenticated
- **Restricting Access:** Preventing forwarding or access to all employee list
- **Secure Email Portal:** Ensuring that messages are not stored on recipients' email servers (which may not be secure) but only within a secure email portal
- **Awareness and Education:** Training for users on appropriate use of email and identifying potentially malicious activity
- **Phishing Campaigns:** Training that helps employees exercise their ability to identify malicious email

Business Email Compromise

- Criminals spoof email communications from executives
  - Initiate unauthorized wire transfers
  - Commonly target businesses that
    - Work with foreign suppliers
    - Regularly perform wire transfers
  - Also known as "CEO fraud"
- Ubiquiti example
  - Tech firm lost $46.7 million in attacks targeting the Finance department
- FBI estimates
  - $2.3 billion in losses over a 2.5-year period

Unexpected incidents can highlight gaps in policy, controls, and business processes. Criminals are conducting an increasing number of "business email compromise" or "CEO email fraud" attacks where they spoof email communications from executives to employees who have the authority to initiate wire transfers. These employees who receive fake emails go about processing unauthorized wire transfers that cost the company, in some cases, millions of dollars. For example, the technology firm Ubiquiti transferred $46.7 million to criminals in an attack targeting their Finance department. This issue has become so widespread that the FBI estimates that companies have lost billions of dollars by falling victim to this attack.

References:
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise
http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

Update Policy to Address Current Risks

Sensitive business transactions, such as wire transfers, must not be completed solely via email authorization.

Verify legitimate requests using additional channels such as a phone.

As the business and threat landscape changes, policy must be updated accordingly. Business email compromise is an issue that requires a change in business process. By analyzing the threats, security can help the business stay informed of current threats and create appropriate policy and controls.

Mobile Device Risks

- Missing security protections
  - Personal devices without security controls
  - Misconfigured devices
  - Insecure mobile apps
- Results in adverse outcomes
  - Data loss
  - Unauthorized access to corporate systems
  - Reputational damage

The first step in policy development is to identify a need. Usually, an individual or business unit identifies a need or a risk; he or she then determines that there is a need for a new or updated policy. This need can be identified as a result of an audit, assessment, or test. Sometimes, the need is identified as a result of a security incident or a breach.

Mobile devices have a number of issues, such as

- Use of personal devices without standard, centralized security controls
- Misconfigured devices that result in a control deficiency
- Use of insecure mobile applications

These issues can result in adverse outcomes such as data loss, unauthorized access, and reputational damage.

Mobile Legal Liability

- Risks of mobile device use while driving
  - Cooley Godward
    - Attorney struck and killed 15-year-old while taking business call
    - She was ordered to pay $2 million and serve 1 year in jail
    - Employer settled $30 million lawsuit for undisclosed amount
  - Solomon Smith Barney
    - Broker struck and killed motorcyclist while picking up phone
    - Employer settled for $500,000
      - They bore "vicarious responsibility" for employee negligence

Jane Wagner, an attorney at the law firm Cooley Godward LLP, was driving her Mercedes while taking a business call. She struck and killed a 15-year-old, Naeun Yoon, and was ordered to pay the family $2 million and serve one year in jail. We mention this, as her employer was also named as a defendant in the lawsuit because she was taking a business call. The firm settled for an undisclosed amount.

Solomon Smith Barney also settled a suit when one of its brokers ran a red light and killed a motorcyclist in Allentown, Pennsylvania while trying to pick up a dropped cell phone. Under the law, companies can bear "vicarious responsibility" if employee negligence causes an accident.

These examples illustrate the importance of having a corporate policy addressing driving and using a corporate-issued or BYOD device where the employee receives a corporate allowance to use his or her personally owned phone for business use.

References:
http://apps.americanbar.org/lpm/lpt/articles/mtt01051.html (link no longer active)
http://www.lexisone.com/balancing/articles/n120102i.html (link no longer active)
https://www.washingtonpost.com/local/trafficandcommuting/employees-use-of-cellphones-while-driving-becomes-a-liability-for-companies/2012/05/20/gIQAFia2dU_story.html

Inappropriate Mobile Device Use: Sexting

- Sexting
  - Sending and receiving sexually oriented messages
  - Primarily between mobile phones via pictures, video, or text
- Risks include
  - Sexual harassment suit, public exposure, brand damage, relationship damage
- Typically, an HR problem with security assistance to
  - Review mobile and access logs
  - Conduct forensics or cleansing of the mobile device

Corporate computing devices may also be used for inappropriate communications like sexting. This can lead to sexual harassment suits, public exposure, brand damage, and relationship damage. Typically, these activities fall under an Acceptable Use Policy and are driven by Human Resources (HR). However, security is frequently involved in reviewing logs, conducting forensics, or cleansing the mobile device.

School Policy Example

Students who are on school property or attending a school event and are caught sharing, viewing or even just possessing sexually explicit material can be punished. The policy applies to both pictures and texts.

In response to the inappropriate use of mobile devices, some organizations, such as the school district of Troy, Michigan, have tried to implement strict security policies around sharing, viewing, and possessing sexually explicit material. This example also highlights how scope can be defined for "students who are on school property or attending a school event."

Reference:
http://patch.com/michigan/troy/new-sexting-policy-allows-troy-schools-to-search-stud079dd74f6d

Mobile Device Search Example

Students and their parents/guardians are hereby placed on notice that in any suspected investigation of a sexting incident, a school official may search a student's cell phone, computer or other electronic device if reasonable suspicion exists that a student has been involved in sexting.

The policy of the school district at Troy, Michigan, went even further by authorizing school officials to search students' mobile devices in the case of "reasonable suspicion" of inappropriate activity.

Reference:
http://www.splc.org/knowyourrights/legalresearch.asp?id=127

What Type of Policy?

- Which flavor of policy would deal with sexting?
  - Establish the bounds of acceptable behavior
  - Encourage employees to do the right thing
- Negative voicing examples
  - "Do not send sexually explicit messages"
  - "Do not respond to sexually explicit messages"
- Positive voicing examples
  - "Electronic messages should be treated like any other form of sexual harassment"
  - "Report inappropriate communications to your manager and/or HR"

This policy would primarily be establishing the boundaries of acceptable behavior, though we certainly would want to encourage employees to do the right thing. Because the goal of this policy would be to protect the company, we might want to be more specific and list some examples and try to be consistent with our voicing.

The One-Sentence Position Statement

- The best policies state the organization's position in a single sentence
  - Similar to a thesis statement
- Mobile examples
  - "Unapproved devices may not be connected to the corporate network"
  - "Mobile devices must always be encrypted"

Ideally, before you start writing the policy, you are able to state the core of the organization's position in a single sentence. You may not be able to cover everything. There may be details, caveats, and use cases, but that one sentence should clearly state what you want the user to know about the organization's position on a given subject.

Think of this statement as similar to a thesis statement. These same tests should apply:

- Your position statement should express the organization's position; "take a stand."
- Your position statement should express one main idea.
- Your position statement should be a foundation for additional discussion.
- Your position statement should be specific enough that people know what you want them to do or not do.

One-Sentence Position Examples

- Acceptable Use
  - "Use your business computer primarily to accomplish the goals of the business."
  - "Do not do anything you would not do if the CEO was sitting next to you."
- Remote Access
  - "Your VPN token is for business use and for your use only; do not share it with anyone for any reason."
- Physical Security
  - "Physical security controls are implemented to protect the company."
  - "Subverting these controls in any way is grounds for dismissal and potential law enforcement engagement."

Here are some examples of one-sentence position statements:

- **Data Classification and Labeling:** Some information is approved and marked as releasable to the public; all other information must be labeled and protected.
- **Data Destruction:** We have a contract with ACME Corp to shred hard drives, CDs, DVDs, USBs; all decommissioned IT equipment from laptops to printers shall go through the process.
- **Digital Signatures:** Keep in mind your digital signature has the same legal standing as your written signature.
- **Economic Espionage:** Economic espionage is the number-one focus of organized crime, closely followed by capturing banking credentials.
- **Electronic Mail:** Before you click Send, make certain that if this message was posted for the whole world to see, you would be proud of it.
- **Employee Surveillance:** ACME employees have no presumption of privacy; we monitor the phone, network, what is stored on local and shared drives. If you have removable media, we reserve the right to scan it, including cameras, USBs, iPhone, and iPads.
- **Physical Security:** Physical security is there for a reason, subverting it in any way is grounds for dismissal and potential law enforcement engagement.
- **Remote Access Policy:** Your VPN token is for business use and for your use only; do not share it with anyone for any reason.
- **User Account Policy:** Access is granted to employees with a business need.

Organizational Position

- Sound out other people such as business unit managers
  - Do they understand the risk?
  - Would they prefer positive or negative voicing?
  - How specific should we be?
  - What are the exceptions?
- Create a clear and simple position statement
  - Avoid obscure language
  - Consider verbally defining policy before putting pen to paper
  - Say it, then write it

"Say it, Then Write It." This is one of the most powerful tips in the course. The worst way to write policy (usually) is to sit down at your keyboard and start pounding away. It looks efficient, but this has led to some very dumb-sounding policy. Say it. See if the other person understands. Then, you are ready to write.

We draft the body of the policy first, because as we explore our voicing and specificity, these things may impact the header. Work from the one- or two-sentence position statement and begin expanding the policy. Try to have natural-sounding policy. One way to achieve this is to get to the point—you can tell people what the policy is. If you make it hard to read, it will not be effective. Users expend minimal effort to understand policy.

If you approach the Legal department early in the game, you reduce the chance of their having problems with the policy later in the process when things are more "public." This part of the process can be tricky. If the Legal department's view is not in sync with the organization's position, you will need to try to broker consensus. One approach is to call a meeting between Legal and the business unit managers. Sometimes, you will find that Legal will suddenly have a new opinion when you do that.

We want to be specific enough but not so specific that a use case we did not think of allows someone to violate the policy. Whenever you use a list, add the language "includes but is not limited to." The procedure test is whether you can build a procedure that gives additional information to someone following the policy. If you can't build a procedure, it is highly probable the policy will not pass the SMART test and is not achievable.

Related Documents

- Mobile Device Policy
- Acceptable Use
- Code of Conduct/Ethics
- Privacy Policy
- Monitoring
- Data Retention and Destruction

For mobile devices, you may decide to have a dedicated Mobile Device Policy. However, clearly, employees must be aware of other policies and documents related to their use of corporate devices. This includes Acceptable Use and the associated Code of Conduct policies.

Typically, organizations will also have Privacy and Monitoring Policies that define the activities the organization conducts to identify inappropriate behavior. This monitoring is also related to the Data Retention Policy, which can limit how far back an investigation can go.

Development Examples

- Acceptable Use
  - Email
  - Mobile
- Secure Development

This page intentionally left blank.

Application Security Issues

- Security vulnerabilities
  - Injection
  - Cross-Site Scripting (XSS)
  - Broken Access Control
- Unpatched dependencies
  - Software supply chain management issues result in vulnerable systems

Again, let's start by identifying the issues that can occur if application security is left unaddressed. It could result in a number of critical security vulnerabilities such as the ones described in the OWASP Top Ten list of most critical web application security risks. These include vulnerabilities like Injection, XSS, and Broken Access Control that have led to data loss, brand damage, and reduced customer trust. Similarly, unpatched third-party software can also expose applications to similar vulnerabilities. This was evidenced with the Struts vulnerability that contributed to the Equifax breach.[1]

Reference:
[1] https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

Secure Development Policy Statement

To mitigate the risk of software security vulnerabilities, we have established policies, standards, and guidelines for the design, development, testing, deployment, and operation of all enterprise software including, but not limited to, web, mobile, desktop, and device-based applications and systems.

To mitigate these risks, your policy should define various activities that need to be injected throughout the software development life cycle (SDLC). Security testing alone is not enough. Security activities need to be injected into the design, development, testing, deployment, and operation of software.

The example above also defines the scope to be web, mobile, desktop, and other applications that are in use in the organization.

Secure Development Standards

Software will be developed in accordance with secure coding standards such as CERT and industry recognized guidelines such as the OWASP Top Ten.

Third-party libraries will be reviewed on a regular basis to ensure that vulnerable components are updated according to risk.

Software development staff (e.g. developers, architects, testers, managers) will attend role-based secure development training on an annual basis.

After the policy statement that defines the high-level activities that need to be conducted, the next level down defines the standards. This gets more specific regarding the secure coding standards that will be used in addition to patching of third-party libraries to mitigate the risk of vulnerable components.

The standard also states that development staff must take the appropriate secure development training on a regular basis.

Secure Development Standards: Protecting Data

Development, test, and production environments must be kept separate.

Production data must not be used for testing or development.

In addition to injecting security into the SDLC, an important mechanism for protecting data is to ensure that production data is never used for development and testing. Many organizations struggle with creating production-like data sets and take the easy way out by reusing production data. As this standard states, this should be prohibited.

Secure Development Guidelines

If you have a security question ask your dedicated security lead. They can describe the issue and can often supply working code that addresses the vulnerability.

If you are on a fast-moving DevOps team let security know so security checks can be automated and the CI/CD pipeline is not slowed down.

Finally, we get to guidelines. These are written in a much more conversational tone because the security team is attempting to build a bridge to the development team. Instead of just forcing a policy and standards for secure coding and training onto the development, these guidelines indicate that security wants to be a partner to development. Going so far as to supply working code and understanding modern DevOps practices goes a long way in building a positive working relationship.

Policy Enforcement

- Penalties for policy violations
  - Define consequences for failing to adhere to policy
  - Can be immediate or phased in over time
  - Enforcement should be related to risk
- Enforcement examples
  - Using personal devices to connect to corporate systems
    - "Access to systems will be revoked"
  - Losing mobile devices
    - "Supervisor will be notified and employee will pay for lost device"
  - Creating applications with insufficient security protections
    - "Annual bonus will be reduced due to lack of quality"

Most organizational policy has a statement that failure to follow this policy can result in discipline up to and including termination. But, if we want people to follow our policy, we need to know what we are going to do if they don't. As we said earlier, the punishment needs to fit the crime, so this is an important discussion to have. Very commonly, HR has the lead on this discussion.

Policy Components

- Ensure the policy has all its parts
  - Purpose, Overview, or Background
  - Scope
  - Policy statement
  - History
    - Publication date, cancellation or expiration, version history
  - Enforcement
  - Responsible parties
  - Related documents or references
    - Other policies, references to compliance standards, glossary

Now that we have developed our policy body, we have probably grappled with issues such as scope, and we should be ready for items like purpose.

- **Purpose or Overview:** Security policy usually contains a statement, often at the beginning, describing the reason the policy is being established and any associated goals.
- **Related Documents:** This section is often titled "References" and usually cites higher-level policy or implementation guidance.
- **Cancellation:** New or updated policy may supersede existing (perhaps outdated) policy. This section identifies those policies and clarifies what is actually in effect.
- **Background:** This optional section provides information amplifying the need for the policy. It may also provide historical information relevant to the subject.
- **Scope:** This section identifies the depth and breadth of coverage (to whom or what the policy applies). Is it for one element of the organization, or will it also apply to contractor agencies who work for your organization?
- **Responsibility:** The security policy document states who is responsible for what. Typical positions that might be addressed include the head of the corporation, the CIO, people in the Legal department or in Human Resources, system administrators, and information security officers. Subsections might identify how additional detailed guidance will be developed and provided in addition to the frequency of policy review. Methods or techniques for measuring compliance may also be included in this section (plus identifying parties responsible for the audit).

Lab 3.2: Vulnerability Management Policy

Estimated Time: 20 Minutes

- Goal of this exercise
  - Identify organizational issues that hinder policy development and adoption
- On your own
  - Take 5 minutes to read the scenario on the next page
- If you finish reading early
  - Start noting key points to discuss with your team

On your own, take 5-10 minutes to read the scenario on the next page.

As you read the case, think about where there are gaps in vulnerability management policy and procedure.

Highlight or underline key items that stand out to you. If you finish reading the case early, start noting key points that you want to discuss with your team.

This scenario has four players:
CEO who runs the company and is being questioned in the aftermath of a large breach
SVP who is a senior IT leader and head of the global platform services team
CSO who is responsible for security governance and is the policy manager
CIO who is accountable for all of information technology

CEO Perspective:
“The individual who was responsible for communicating in the organization to apply the patch did not. We get notifications routinely, the IT team and Security team do, to apply patches. This individual, as I mentioned earlier, did not communicate to the right level to apply the patch. I described it as a human error where an individual did not ensure communication got to the right person to manually patch the application. That was subsequently followed by a technological error where a piece of equipment we use which scans the environment looking for that vulnerability did not find it.”

SVP Perspective:
“I was just one of 430 employees to whom the vulnerability email alert was sent. I am copied on this email for informational purposes, but no specific action was required of me because I don’t have specific responsibility under the patch management policy. I'm not a system owner or an application owner.”

CSO Perspective:
“My Security team had global responsibility and would establish the policies and the standards, or the rules, which the IT team would operate under. And so when you mention specific systems, that makes me think of the IT team, who is responsible for following the rules that the Security team has set forth. So we had a working relationship where security would establish the rules and work with the IT team to implement those rules.”

CIO Perspective:
“I don’t believe there was any explicit designation of business or application owners. My guess would be that the system owner would be someone in the infrastructure group probably under the SVP, since as part of the global platform services group, his team ran the sort of server operations.”

Asked if it would the SVP who would have been the one responsible for actually applying patches, the CIO replied:

“Possibly. Again, we are talking at a level that I wasn’t involved in, so I can’t talk specifically about who actually had physical access to that system to be able to install the patch. I did not have a specific role or responsibility to patch the system as a senior executive and was a manager of managers who managed teams that would fulfill roles laid out in the policy.”

==

Scenario is based on slightly modified information from the Congressional Equifax Breach Report.[1]

Reference:
[1] https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Lab 3.2: Group Discussion

- As a group, discuss the following questions:
  - How would you describe the current state of security?
  - What policy and related documents need to be put in place?
  - What are five roles and the corresponding responsibilities that should be formally defined?
  - What are three things that can be done to make vulnerability management a regular business process?

NOTE

Don't read the next section yet

It contains a debrief and potential lab answers

As a group, discuss the following questions:

1) How would you describe the current state of security?

2) What policy and related documents need to be put in place?

3) What are five roles and the corresponding responsibilities that should be formally defined?

Role #1:

Role #2:

Role #3:

Role #4:

Role #5:

4) What are three things that can be done to make vulnerability management a regular business process?

#1

#2

#3

Vulnerability Management Policy Debrief

Note that this section contains a debrief and potential lab answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after the group discussions have taken place.

Current State of Security

- Lack of leadership
  - "This individual as I mentioned earlier did not communicate to the right level"
- Siloed
  - "When you mention specific systems, that makes me think of the IT team, who is responsible for following the rules that the Security team has set forth"
- Fragmented
  - "I was just one of 430 employees to whom the vulnerability email alert was sent"
- No accountability
  - "I'm not a system owner or an application owner"
- Unclear responsibilities
  - "My guess would be that the system owner would be someone in the infrastructure group probably under the SVP"

There is a clear lack of leadership in this case. The CEO specifically blames a single individual for not forwarding an email. Certainly a robust enterprise process would not depend on a single individual remembering to forward an email. Part of the problem was that security responsibility was siloed across the organization. The CSO states that her team simply made the rules and IT was supposed to follow them. Not much collaboration happening based on that statement. Moreover, responsibility is fragmented. Over 430 people receive an email alert? If everyone is responsible then no one is responsible. This lack of accountability is clear when the SVP states that "I'm not a system owner or an application owner." These unclear responsibilities are evident in multiple comments where people "guess" who is the owner.

Policy Set for Vulnerability Management

- Policy
  - State high-level vulnerability management policy statement
  - Define vulnerability management targets and roles and responsibilities
- Standard
  - Define requirements for vulnerability scanning, risk rating and prioritization, and remediation deadlines
- Procedure
  - Define steps that will be taken by responsible parties related to notification of vulnerabilities, remediation tracking, and risk acceptance

In this debrief, we will discuss elements of a vulnerability management policy, standard, and corresponding procedures.[1]. These sample documents are available in the course Digital Download Package online at mgt514.com in the Section 3 -> Vulnerability Management directory.

From the scenario, it is clear that while there may be a policy in place, there is not a clear definition, agreement, or execution of roles and responsibilities. Having a high-level statement—"To safeguard the information with which we have been entrusted, information systems personnel must take active steps to discover and remediate software vulnerabilities on a recurring basis"—is a good first step, but it needs to also define agreed upon remediation targets.

A vulnerability management standard helps make the policy more concrete by defining specific requirements for vulnerability scanning, risk rating and prioritization, and specific remediation timelines.

Finally, the vulnerability management procedure should define actions of responsible parties related to communication, notification, remediation tracking, and risk acceptance.

Reference:
[1] Vulnerability management policy, standard, and procedures were created by Daniel Tabor (dtabor1@gmail.com)

Set a Target

Based on the organizational risk appetite for software vulnerabilities, personnel should strive for **100% on-time remediation** of externally exploitable vulnerabilities which could lead to code execution and **85% on-time remediation** of all other vulnerabilities.

Here is an example of setting targets for vulnerability management. This example policy fragment states that "personnel should strive for 100% on-time remediation of externally exploitable vulnerabilities, which could lead to code execution." It is important to note the word choice here. The phrase "should strive for" is used specifically to give the organization some leeway in accomplishing this task while also helping to highlight the importance of vulnerabilities which could lead to code execution. The policy fragment then goes on to state that all other vulnerabilities should have 85% on-time remediation. Again, the critical part here is defining a concrete goal that can be measured.

Define Roles and Responsibilities

- CISO
  - Security executive accountable for determining risk appetite and setting policies and procedures to manage risk
- Business Owner
  - Executive leader responsible for business risk and approving remediation of security vulnerabilities
- System Owner
  - IT leader responsible evaluating and applying patches to remediate vulnerabilities
- Application Owner
  - Development leader responsible for secure coding practices and to fix vulnerabilities
- Vulnerability Management (VM) Team
  - Responsible for scanning, risk rating, communicating status, tracking and remediation

The following are example roles and responsibilities for vulnerability management.

Chief Information Security Officer (CISO): The CISO is accountable for determining the organizational risk appetite and setting information security policies and procedures in accordance with that appetite.

Business Owner: The business owner of an application or information system is the executive leader responsible for the primary business process served by that application or information system. The business owner is responsible for understanding the business risks posed by unauthorized disclosure, loss of availability, or loss of integrity to the data in the system. They are also responsible for approving maintenance windows as appropriate for remediation of security vulnerabilities.

System Owner: The system owner of an application or information system is the IT leader responsible for operations and maintenance of the application or information system. The system owner is responsible for evaluating and planning for the impact of security patches to the information system. They are responsible for applying patches to remediate vulnerabilities within acceptable timeframes.

Application Owner: The owner of an application is the development leader responsible for the ongoing development of the application. They are responsible for ensuring that security objectives for the application are met, including secure coding practices and timely issuance of updates needed to fix security vulnerabilities.

Vulnerability Management (VM): The VM team is responsible for scanning systems to detect the existence of vulnerabilities; providing risk ratings for new vulnerabilities; communicating vulnerability status to business, system, and application owners; tracking the remediation status of observed vulnerabilities; and ensuring remediation occurs within defined service level agreements.

Institutionalizing Security

- Change reporting relationships
  - Security responsibilities are siloed
  - Governance & policy report to CSO but technical security teams report to IT
  - Elevate importance of security by having CSO report to CEO or CRO
- Define a single point of responsibility
  - No one was responsible for vulnerability management
  - Define a central leader and team with responsibility and executive mandate
- Tie security goals to compensation and/or bonuses
  - Define clear vulnerability management goals and targets
  - Align these targets with organizational strategic objectives
  - Set monetary impacts if goals are met

As we saw from the case, security responsibilities were siloed. The full case states that the CSO reported to the General Counsel and that there was a contentious relationship with the IT team that oversaw technical security activities.[1] This led to a gap between the governance and policy team under the CSO and the technical teams charged with implementation. To remedy this situation, especially in a large organization, it would be beneficial to elevate the importance of security by changing reporting relationship to have the CSO report to either the CEO or someone at the level of a Chief Risk Officer (CRO).

No one was responsible for vulnerability management. However, it's not enough to identify a central leader and team. More importantly, this team must have an executive mandate to drive change and obtain buy-in from various business units that will likely resist efforts to remediate vulnerabilities more aggressively.

One way this can be done is by linking security goals to executive compensations and bonuses. Defining clear targets in the vulnerability management policy and setting monetary impacts if the goals are met (or not met) incentivizes executives to prioritize security.

Reference:
[1] https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- ***Manage Policy***
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

Define Roles

- Identify key stakeholders
  - Legal, HR, Operations, Business Units
- Solicit feedback during development
  - Informal review will be beneficial

> At appropriate times during drafting of the policy, the document is shared with Stakeholders for their comment. The Responsible Office, in consultation with the Responsible Executive, considers all feedback and determines whether and how to incorporate it.

Engage the following stakeholders as you develop policy:

- **Executive Management:** Organizational leaders need to fully understand directives and laws that form the basis for the security program. They also need to comprehend their leadership roles in ensuring full compliance by users within their units. Policy is a tool to help them govern.
- **Security Personnel (security program managers and security officers):** These individuals act as expert consultants for their organization and, therefore, must be well educated on security policy and accepted best practices.
- **Business Unit Managers:** These managers must have a broad understanding of security policy and a high degree of understanding regarding security controls, regulatory compliance, and requirements applicable to the business they manage.
- **System Administrators and IT Support Personnel:** These individuals are entrusted with a high degree of authority over support operations critical to a successful operation; they need a higher degree of technical knowledge in effective operations and security practices and implementation.
- **Lower-Level Operational Managers and System Users:** These individuals need a high degree of security awareness and training on security controls and rules of behavior for systems they use to conduct business operations. They have the credentials to access proprietary data, and what they can and cannot do should be controlled to the extent possible.

Draft the body of the policy and present it for informal review. Remember, a person who is not familiar with the subject the policy covers is an ideal person to do the informal review.

Reference:
https://www.purdue.edu/policies/governance/vc1_procedures.html

Define Approval Process

- Identify stakeholders required for approval

With the Responsible Office's approval, the policy draft and a completed needs assessment are submitted to the **Policy Committee** for comment.

With the **Responsible Executive**'s approval, the final draft is distributed to the Executive Council for review.

The **Executive Council** makes a determination on the policy.

If **Board** approval of the policy is necessary, the **Chair** of the Executive Council will forward the policy document to the **President**.

A good career tip is to get some people who know you to look at the policy before sending it to stakeholders like the business unit managers and chief executives. People are busy and do not always read email thoroughly. Consider printing the policy and having the policy review as part of a meeting. Be respectful of others' time; it is far better to do policy review as part of a general-purpose meeting than call a meeting just to review policy. You may have to attend several meetings, for instance, one with the business unit managers and another with the people responsible for governance, such as the chief executives and the board. That is okay, too. Unless there is contention, it should not take more than 10 minutes to read, discuss, and review a page-and-a-half-long policy. If you do have a situation in which people have strong and differing opinions, it is much better to find this out before the policy is sent to the rank and file.

Run the policy by Legal before sending it out for approval. Lawyers have a lot of practice at reading documents and considering details, and you certainly do not want to have problems with the policy pointed out in front of the senior executives. So, you work with Legal twice during the process: First, to get guidance (what should the policy say or not say); and second, to review the draft (but ready-to-send-to-the-executives policy).

Complete the entire policy and submit it for review and revisions. Many companies have complex policy review processes and require as much as a year to complete policy review. In some organizations, board-level review is needed. This is because policies are the statement of intent of senior leadership about the organization’s security posture. However, rarely will the board conduct a line-by-line review of the policy. The board will typically rely on subcommittees and delegates to perform the review and provide a recommendation.

Reference:
https://www.purdue.edu/policies/governance/vc1_procedures.html

Socialize the Approved Policy

- Distribute and communicate about new policy

  All approved policies will be published on the **official company policy site**. Any policy published on or linked from the official policy site must include a reference to the employee or department responsible for updating the policy.

  In order to promote consistency, policies will be housed in a common **enterprise web content management system**.

  Approved policies may be distributed using a variety of methods including **email**, notice through department **websites**, notice through the corporate **newsletter**, and/or distributing **hard copy**.

After policy is approved, it needs to be distributed to all parties affected. It's time for an authorized person to sign it and put it in place. There should be mechanisms such as email notifications, so that all employees, contractors, or customers covered by the scope of the policy are notified of the policy.

Document management is very important. Issues of file sharing, document storage, and version control need to be addressed.

Policy Awareness and Training

- Awareness
  - Description of risks
  - New employee onboarding
  - Annual awareness training
  - Regular quiz on key elements of policy
  - Tip of the day
- Training
  - Provide skills so people can follow the policy
  - Outline procedures that support the policy
  - Instruct where to go for additional support

The company will provide training on how to handle personal information appropriately as part of their job responsibilities.

One use of awareness programs is to inform users about policies. Or, perhaps they know about a policy, but they think it is silly because they do not know the risks involved. Awareness programs can tell them about the risks and why it is in their best interest to follow the policy. Sometimes, users might need training to develop the skills to follow the policy, or more likely, the procedures that support the policy.

A quiz can be designed not just to assess, but to teach and reinforce.

Measuring Policy

- Monitor adherence to policy
  - Regularly audit and report on violations

> The company must perform regular monitoring to ensure that the information security program is operating in a reasonable manner to prevent unauthorized access to or unauthorized use of personal information.

How do you know if policy is being followed? Regular audits and monitoring help detect policy violations. In some organizations, the Internal Audit department serves this function and reports to the board on the current state of compliance.

Enforcement: Responsibilities Example

- Who enforces the policy?

> **Users** are required to responsibly and securely maintain and use institutional data that they store on the Box service, sync onto any device, or share through the service.
>
> It is strongly recommended that individuals create their own personal Box account independently from the Box service, rather than store personal data in their Box account. **Managers** have the authority to limit the personal use of institutional systems.

In addition to audit, it is also useful to empower users to enforce controls on themselves by utilizing services responsibly. This example, which likely takes into account the organizational culture of openness and collaboration, also leaves it up to managers to limit use as necessary.

Reference:
https://it.tufts.edu/boxpol

Enforcement: Consequences

- What happens if you don't follow the policy?

> Individuals who store personal data in their Box account will **cease to have any access to that data** upon the termination of their employment.
>
> It is solely the individual's responsibility to remove any and all such personal information from the Box file before the end of their employment. **The company will have no responsibility to provide any such information** to the individual after such termination or to continue to store such information.

Policy must also include consequences of sanctions in the event of noncompliance. In this example, the consequences are straightforward: You will lose access to personal data that is stored online when you are terminated. Personal data is entirely your responsibility and the organization has no responsibility to provide access to personal data after termination.

Reference:
https://it.tufts.edu/boxpol

Exception Requests

- Reason for exceptions

> Situations or scenarios will arise that cannot be effectively addressed within the constraints of existing security policies and standards. There will be times when business processes can and should take precedence over these policies. Therefore, a review process is provided to approve and document requests for exemptions to policy. The process allows leadership to make an informed decision on whether or not to request an exception to a particular IT policy by understanding the risk and alternatives involved.

Sometimes, new business processes or technologies require changes to policy. A policy exception is a gap between the adopted security policy and the actual state of security controls. A process that allows the organization to review exception requests enables the organization to make changes over time. A flood of exception requests for similar items likely means that policy is outdated and needs to be updated.

Reference:
http://policylibrary.gatech.edu/policy-exceptions (link no longer active)

Handling Exception Requests

- Exception process
  - Review business justification
  - Assess risk
  - Identify compensating controls
  - Approve (or reject) exception
  - Communicate results
- Ensure that a business owner or sponsor signs off on the risk
  - Security merely advises on risks and controls
  - Keeps security from being a bottleneck
  - Made easier by including multiple use cases in the policy itself

Exception requests should include the following:

- **Business justification:** Describes the value that the new process, technology, and so on will bring to the business
- **Assessment of risk:** Identifies the additional risk introduced if the exception were to be approved
- **Compensating controls:** Identifies compensating controls that can mitigate the risk

After a decision has been made on the exception request, it should be clearly communicated not only to the requestor but also to all interested stakeholders.

Often, the Security team is the group that reviews and approves or rejects exception requests. This puts Security in the position of being a bottleneck or blocker. A better approach is to have a business owner or sponsor sign off on the risk. This puts Security in a position of merely advising on the risks and controls. This approach is also made easier by considering all use cases when developing the policy. If you reduce the potential number of exception requests ahead of time, there will be fewer opportunities for Security to block.

Expiration Date

- Can define a specific expiration date
  - Usually based on the approval date

> The exception will be granted for a period of no more than **one year** from the time the exception is granted. At the end of the year, the exception will be reviewed and either terminated or renewed for another period.

- Or define a global review period

> Security policies will be reviewed **annually** or as required by relevant external regulation.

Policy needs to be reviewed regularly to determine if the risk is still valid and whether the controls work. It also needs to be reviewed to identify additional controls and review known violations.

Policy should be reviewed and rewritten when changes occur, annually or at least biannually. Naturally, anytime you have a policy that covers a given subject and an event occurs such that the policy does not give guidance, it is time to review the policy.

In some organizations, you may not need a full stakeholder review to reapprove policy. A policy committee may review the policy to see if it needs to be updated. If the risk is still valid and a control assessment validates that the controls work and there are no available additional controls, then the committee can probably reapprove the policy for another year or two. If additional appropriate controls are available, maybe they can be specified in a procedure.

In smaller organizations, a manager may even be able to reapprove the policy after the annual review based on a global review period.

Reference:
http://policylibrary.gatech.edu/policy-exceptions (link no longer active)

Soft Expiration Date

Every policy will be reviewed **periodically** by the CISO or delegate. The CISO will make or propose modifications on an as-needed basis to keep the policy current. The document history must include the initial effective date and the last amended date.

Policies may be modified **whenever necessary** to comply with regulatory changes or changes in business operations. Policy modifications will follow the same review and approval process as for new policies.

In some cases, organizations may not want to put a hard expiration date on each policy. Instead, policy can still define a review period of "periodically" or "whenever necessary." If such soft expiration dates are used, it is important that the reviews actually occur to enforce life cycle thinking and incorporate new business requirements into the approved policies.

Policy Life Cycle Management

- Expiration date is required to ensure a life cycle approach
  - Update policies based on evolving business requirements and threats
  - Technology changes require revisiting policies
    - Modem policy example

> The risk is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers from within the corporate network, then there is the possibility of breaching the internal network through that computer, unmonitored.

We use this fragment of a modem policy to show why an expiration date might be a good tool. As technology changes, the risks change. Without an expiration date, a policy like that could remain in the system a long time. Would that be a real danger to an organization? No. However, if we want people to follow policy, we need to do our part to make sure it is relevant.

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - ***SMART Approach***
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

SMART Approach

- Specific
  - Targets a specific area
- Measurable
  - Can be quantified to show progress
- Achievable
  - Is attainable and action oriented
- Realistic
  - Can be achieved using available resources
- Time Based
  - Defines what can be achieved in a given time period

The key to good policy is specifics—not in the sense of how to do things step-by-step; that is the responsibility of procedures. Rather, the policy has to be clear enough so that you can create the procedures to support it. The SMART approach to policy is based on a framework of being Specific, Measurable, Achievable, Realistic, and Time Based. We will cover each of these in turn.

How Specific Should Policy Be?

- Specificity depends on the organization
  - Procedure can usually be approved more quickly
  - Move specifics to the procedure if policy approval time is long
- Level of specificity also depends on the type of policy

> Secret: Information requiring a substantial degree of protection. The unauthorized disclosure of secret information could reasonably be expected to cause serious damage to national security.

The amount of specificity that you put into policy depends on your organization. How quickly can your organization approve changes to policy? If the policy approval process is extremely long, then you will want to put more of the details into the procedures. However, if policy can be approved very quickly, it may be acceptable to have more details in the policy itself. This is usually the case with smaller organizations.

When you're looking at specific policy documents, the level of specificity also depends on the type of policy. For example, a high-level policy describing the types of data and associated data classification is usually, by definition, more general, as is shown by the "Secret" policy fragment above. It very broadly defines "information requiring a substantial degree of protection" that could "cause serious damage to national security." Very general. However, the policy can then go on to include more specific examples from which procedure can be defined.

General or Specific and Why? (1)

Equipment which is working, but reached the end of its useful life will be made available for purchase by employees. A lottery system will be used to determine who has the opportunity to purchase available equipment.

All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.

Finance and Information Technology will determine an appropriate cost for each item

All purchases are final. No warranty or support will be provided with any equipment sold.

This policy is specific. Why? Because letting employees buy used equipment, although a benefit, can have a number of pitfalls. Some of the risks include internal fraud, taking equipment instead of going through the policy, disagreements about someone being favored, hence the lottery. Clearly, this organization has anticipated some of the potential problems (or modified its policy after problems have developed).

Reference:
https://www.sans.org/information-security-policy/?category=server_security

General or Specific and Why? (2)

IBMers are personally responsible for the content they publish online, whether in a blog, social computing site or any other form of user-generated media. Be mindful that what you publish will be public for a long time—protect your privacy and take care to understand a site's terms of service.

Identify yourself—name and, when relevant, role at IBM—when you discuss IBM or IBM-related matters, such as IBM products or services. You must make it clear that you are speaking for yourself and not on behalf of IBM.

If you publish content online relevant to IBM in your personal capacity use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent IBM's positions, strategies or opinions."

These fragments from IBM's social media guidelines are very specific. This example is used to highlight that, although policy may be more high level, other documents like guidelines or procedures can get into more detail and provide specific actionable guidance for employees.

Reference:
https://www.ibm.com/blogs/zz/en/guidelines.html (link no longer active)

General or Specific and Why? (3)

All political activities on employer's premises during work-time are prohibited

The use of the organization's name, logo, email, and file systems in connection with any political group or activity is prohibited

Employees wishing to run for political office must discuss it with management prior to announcing their candidacy so the employer can determine what is allowed during work time

The first fragment above is very general. The next two fragments are quite specific.

References:
http://hr.blr.com/HR-news/Performance-Termination/Political-Activity-Workplace/Creating-Workplace-Policies-on-Political-Activity (link no longer active)
http://www.bizfilings.com/toolkit/sbg/office-hr/managing-the-workplace/workplace-rules-should-address-employee-politics.aspx

How to Make Policy Measurable

- Policy focuses on high-level goals
- Procedure focuses on step-by-step instructions
- Focus on measurable outcomes
  - Help bridge the gap between policy and procedure
  - Essential outcomes can be tracked and enforced

When policy is specific, it is usually measurable. Policy tends to define high-level goals, whereas procedure is very detailed in providing step-by-step instructions to meet various goals. A good tip for making policy measurable is to define measurable outcomes, not in the policy itself, but as part of your process for developing policy. Defining measurable outcomes helps bridge the gap between policy and procedure, enabling you to track and enforce key outcomes.

Less Measurable

Failure to Abide by Third-Party Website Policies
Violating the rules, regulations, or policies that apply to any third-party network, server, computer database, or website that you access.

This example is very general. By definition, it is impossible to track all third-party website policies and determine whether or not your users are actually abiding by them.

Reference:
https://paysimple.com/acceptable-use-policy

Very Measurable

The Idaho Youth Ranch will operate on the security principle of "that which is not explicitly allowed is explicitly denied."

Attempts by anyone to access, monitor, use or share information that is not explicitly allowed to them by our security program will be considered a security violation. Further, access to sensitive information will be permitted on a "need to know" basis, such that employees have access to only those data and systems required to perform their assigned jobs.

We will deploy systems, processes, policies, and training to protect our mission-critical data assets and customer privacy. Most important, we will monitor and enforce compliance with our policies.

The Idaho Youth Ranch is a nonprofit that offers services for at-risk children and their families. Due to the sensitive nature of the work, the company has a philosophy that "puts securing our customers' personal data as one of the company's highest priorities." That is evidenced in its security policy above, which defines a strict need-to-know approach for data access. This strict access control and the systems, processes, and training it utilizes can all be measured against the goals and outcomes it has defined for the program.

Reference:
http://www.youthranch.org/security-policy

Achievable (1)

Once the data and application requirements are established, computer security personnel can then evaluate risk and determine methods, processes, equipment, and procedures to mitigate known risks.

This policy fragment is very vague. It basically states that after requirements are created and a risk assessment is conducted, the Security team will define appropriate security controls to reduce risk. In general, this is achievable, but it is not very specific or measurable, which can make it difficult to achieve.

Reference:
http://www.comptechdoc.org/independent/security/policies/application-implementation-policy.html (link no longer active)

Achievable (2)

The computer security personnel, customers, and application developers will work together to provide required and reasonable access capability to systems and data both during development and final project implementation while providing the best computer security possible for a reasonable cost.

Now, we try to get a little more specific by defining who will work together to reduce risk. However, this policy is still too vague. How will security and development work together? Is that even possible when they are trying to "provide the best computer security possible for a reasonable cost?"

Reference:
http://www.comptechdoc.org/independent/security/policies/application-implementation-policy.html (link no longer active)

Realistic (1)

All employee use of the internet must be for business purposes only.

"The internet must be used primarily for business purposes. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of the internet. If there is any uncertainty, employees should consult their supervisor or manager."

Reference:
http://www.comptechdoc.org/independent/security/policies/internet-connection-policy.html (link no longer active)

Realistic (2)

Computers must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. For example, installations that allow unrestricted access to resources must be configured with extra care to minimize security risks.

Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk

Attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus or off-campus resources, including computers maintained for a small group or for an individual's own use.

It is realistic to require computers to have recent patches along with appropriate authentication and authorization. However, this high-level policy fragment does not define when those patches would be installed. Depending on the service level agreement (SLA) certain deadlines may or may not be realistic. Further details need to be clarified in the corresponding standards and procedures. Additionally, highlighting small systems as well as large systems is likely based on the policy writer's insight into the actual operations of this organization. The phrasing of this statement provides some leeway as it does not specify how much attention must be given to these various systems.

Time-Based (1)

Account termination: The supervisor of a terminated employee must notify IT of the separation on or before the employee's termination date so that account access can be revoked appropriately.

Not clearly defining a time component is one of the most commonly neglected items when policy is being created. As a result, the time component is most often identified as an issue when using the SMART approach. Having said that, when it is really the job of procedure, terms like "on or before" or "immediately" are fine in policy as long as they are supported by procedure.

Note: The term "on or before" does not leave much wiggle room. If a supervisor does not report and a malicious or disaffected employee causes harm, the supervisor is in a bit of a jam. A better approach would be to suspend access immediately (it can always be added back). Also, you may want to audit what access is needed for the remainder of the time the employee will be working and assign a shadow to learn his or her job tasks.

Reference:
http://www.ecu.edu/prr/08/05/05

Time-Based (2)

Backup: Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

This policy fragment is nicely done. By naming dates, it is measurable.

Reference:
http://www.comptechdoc.org/independent/security/policies/backup-policy.html (link no longer active)

SMART Exercise #1

Timely signature updates should be available from the vendor. No more than one week should pass between a vendor's release of new signatures and the application of these new signatures.

A change management procedure specifically designed for signature updates should be developed and followed.

Specific: Specific enough to develop procedures and define measurable outcomes.

Measurable: The percent of systems that have up-to-date signatures and the number of systems meeting signature deployment SLAs can be easily measured.

Achievable: Deploying new signatures on a regular basis is very achievable.

Realistic: Developing a change management procedure is realistic. Assuming that "timely" signature updates are delivered by the vendor may not be so realistic.

Time-based: Weekly deployment of new signatures very clearly lays out the time.

SMART Exercise #2

All encryption must be done using NIST approved cryptographic modules.

Common and recommended ciphers and protocols include AES, RSA, SHA-512, SHA-3, TLSv1.1, and TLSv1.2.

Symmetric encryption must be at least 128 bits. Asymmetric encryption must be at least 2048 bits.

Key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.

Specific: Very specific. Probably too specific for a policy. Details of specific algorithms such as AES and RSA should be left for a standard.

Measurable: A review or audit can be conducted to identify areas that are not using NIST-approved cryptographic modules.

Achievable: Yes, very achievable.

Realistic: The upgrade "as technology allows" helps make this realistic as there are some situations that may require the use of older ciphers or protocols.

Time-based: This clause is about annual review accounts. The company can also consider reviewing the list of NIST-approved cryptographic modules whenever it is updated.

SMART Exercise #3

Weak passwords are passwords that are easily guessed or broken by a determined attacker. Some characteristics of a weak password are

- Any password having fewer than eight characters
- Passwords that include single dictionary words in any language
- Names or initials of family members, friends, or pets
- Birth dates, and/or other significant dates
- Recognizable patterns of words, numbers, or symbols (qwerty, 12345, !@#$%)
- Any of the above in reverse or with a number or symbol added to the beginning or end
- Any password that is cracked using the procedures authorized in the auditing section of this document

Specific: Yes, as this password standard defines specific characteristics that should be avoided.

Measurable: Systems and configuration can be reviewed to ensure that passwords meet these characteristics.

Achievable: Yes, overall achievable. However, it is not possible to have technical mechanisms to detect the use of family members, friends, or pet names.

Realistic: Yes, it is realistic to have this password standard and certain guideline elements.

Time-based: No mention of time.

SMART Exercise #4

Employees may not install software on company computing devices operated within the corporate network.

Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email.

Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.

Specific: Specific enough to define the overall goal (preventing installation of any software) and a high-level process for requesting new software.

Measurable: Installation attempts and software requests can be tracked to measure the impact of this policy.

Achievable: Users might not be happy, but centrally managed endpoints can be set up to prevent installation of any new software.

Realistic: Assuming that this policy is for a closed organization, this could be a realistic policy. However, in a more open organization, how long will users wait if "no selection on the list meets the requester's need"?

Time-based: No mention of time. When will IT or the Help Desk get back to the requester? This may be pushed to more detailed procedures.

SMART Exercise #5

Corporate offices must retain a proof of destruction for agencies requiring such. At a minimum, the proof of destruction must provide:

- The serial number of the storage media device
- The date of media destruction
- The method(s) used to destroy the media (for example, pulverizing, shredding)
- The vendor's name if a vendor was used to pick up and/or destroy the storage media
- The name, title, and signature of the person who supervised the destruction of the storage media device

Specific: Very specific. Some items may be so specific that they can be pushed to a procedure.

Measurable: Percent of destruction requests without appropriate documentation can be easily tracked.

Achievable: Yes, very achievable. However, a process would need to be in place to ensure that vendors also follow this policy.

Realistic: Very realistic.

Time-based: No mention of time.

Reference:
http://www.utahta.wikispaces.net/file/view/5000-0001+Removal+of+Data+20101214+revised.pdf (link no longer active)

Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - ***Policy Assessment***
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.

This page intentionally left blank.

End of Round 2

- Round 2 scoring adjustments
  - For every $250k spent beyond your budget
    - Decrease Security Culture by 1 point
  - For every 1 time unit spent beyond your plan
    - Decrease Security Culture by 1 point
  - For every 1 point greater than three for each Security Function dial
    - Increase Security Culture by 2 points

For each Round of play the Security Culture score is adjusted.

For every $250k spent beyond your budget decrease your Security Culture score by 1 point. For example, if you have a -$500k budget then decrease Security Culture by 2 points.

For every 1 time unit spent beyond your budget decrease your Security Culture score by 1 point. For example, if you have -4 time points then decrease Security Culture by 4 points.

For every 1 point greater than three for each Security Function dial increase Security Culture by 2 points. For example, if your Decipher dial is 4 and your Develop dial is 5 then increase Security Culture by 6 points.

CYBER42

Event #9

Debrief

This page intentionally left blank.

Lab 3.3: Cloud Computing Policy

Estimated Time: 20 Minutes

- On your own
  - Take 10 minutes to read the 2.5-page policy
- As you read the policy, think about
  - Risks PharmaCo is trying to address
  - Scope of the issue
  - Language and structure of the policy
- If you finish reading the policy early
  - Start noting key points to discuss with your team

PHARMAC

On your own, take 10 minutes to read the 2.5-page Cloud Storage Policy. As you read the policy, think about the risks PharmaCo is trying to address, the scope (that is, to whom this policy should apply), and the language and structure of the policy. If you finish reading the policy early, start noting key points that you want to discuss with your team. When everyone is done reading, discuss with your team members.

Cloud Storage Policy
Purpose:
This policy outlines best practices and approval processes for using cloud storage services to support the processing, sharing, storage, and management of corporate data at PharmaCo.

Scope:
All PharmaCo employees.

Overview:
Cloud storage services are provided by companies such as Box, Dropbox, Google (Drive), and Microsoft (OneDrive). These cloud computing services are generally easy for people and organizations to use, they are accessible over the internet through a variety of platforms, and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

Policy Statement
Considerations for Cloud Computing Services:
Most cloud services make it easy for individuals to sign up and use (self-provision) their services via an End User License Agreement (EULA), often at no monetary cost. PharmaCo also locally or centrally acquires cloud services for use by employees.

Employees must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise, manage corporate data (as defined by the Data Protection Policy). Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

Risks of using self-provisioned cloud services include:
- Unclear and potentially poor access control or general security provisions

In contrast, PharmaCo negotiates agreements with service providers for locally and centrally provisioned services. The terms of these services are more clearly defined and well known by the company. In short, centrally provisioned cloud services are vetted environments whose risks are better measured and accepted by PharmaCo.

Procuring or Licensing Cloud Computing Services:
If your division, department, office, or lab is looking to provision cloud services to support its work, the first step is to consult with its Information Steward(s) and Contract and Licensing Services.

Employees must not self-provision cloud services to store, process, share, or manage Level A: Regulated Data. Defined by the Information Classification and Handling Policy, regulated data are data that are regulated by information privacy or protection laws, regulations, contracts, binding agreements (such as nondisclosure), or industry requirements. If your division, department, office, or lab needs to provision a cloud service to store, process, share, or otherwise manage regulated data, it must work with Contract and Licensing Services in order to properly evaluate and manage the risks that come with using the service for regulated data.

Confidentiality Level	Description	Cloud Use
Level A: Regulated Data	All data that is governed by privacy or information protection mandates required by law, regulation, contract, binding agreement, or industry requirements.	Must not use self-provisioned cloud services to store, process, share, or otherwise manage regulated institutional data without working with Contract and Licensing Services to develop the appropriate contractual safeguards. Must use only a contractually (locally or centrally) provisioned cloud service once you have confirmed with your Information Steward or Contract and Licensing Services that the service is appropriate for confidential institutional data. Not all centrally and locally provisioned services are designed to handle regulated data.
Level B: Confidential Data	Data that is meant for a very limited distribution – available only to employees on a strictly need-to-know basis.	Should not use self-provisioned cloud services to store, process, share, or otherwise manage confidential data without ensuring that a service's safeguards are appropriate for confidential data. Should only use a centrally or locally provisioned cloud service once you have confirmed with your Information Steward that the service is appropriate for confidential data. Not all contractually provisioned services are designed to handle confidential data.
Level C: Administrative Data	Data that is meant for a limited distribution; available only to employees that need the data to support their work. This data derives its value for PharmaCo in part from not being publicly disclosed.	Should not use self-provisioned cloud services to store, process, share, or otherwise manage administrative institutional data without ensuring that a service's safeguards are appropriate for administrative data. Should use only a centrally or locally provisioned cloud service once you have confirmed with your Information Steward that the service is appropriate for administrative data. Not all contractually provisioned services are designed to handle administrative data.
Level D: Public Data	Data that is intended for wide and open distribution to the public at large. This data does not contain confidential information.	May use self-provisioned cloud services to store or manage public data with caution. Should ensure that using these cloud services does not violate any licensing agreements. May use contractually provisioned cloud services to store or manage public data.

Approval Date:
January 11, 2021

Review Committee:
Information Risk Steering Committee
IT Executive Council

Revision:
PharmaCo reserves the right to change this policy from time to time. Proposed changes will normally be developed by the policy managers with appropriate stakeholders. The Review Committee has sole authority to approve changes to this policy.

==

Note: This policy is a modified version of the Cloud Computing Services Policy from Tufts University. https://it.tufts.edu/cloud-pol

Lab 3.3: Group Discussion

- As a group, discuss the following:
  - Define scope
    - How can the "Scope" section be made more comprehensive?
  - Provide background
    - What part of the "Overview" section is very specific? Why?
  - Identify risks
    - What is the primary concern in the "Procuring" section?
    - What risks are missing from the "Considerations" section?
  - Language of policy
    - Why did the author use certain words in the "Cloud Use" column?
  - Policy structure
    - What items are missing from the policy footer?

NOTE

Don't read the next section yet

It contains a debrief and potential lab answers

As a group, discuss these five items:

1) **Scope:**
   The "Scope" section simply says "All PharmaCo employees." How can it be improved and include information about which cloud services are in scope?

2) **Overview:**
   Review the "Overview" section. Some parts are very specific. For example, it specifically calls out "Apple, Google, Microsoft, and Amazon." Why do you think the policy goes into that level of detail?

3) **Identify Risks:**
   The "Procuring or Licensing Cloud Computing Services" section defines a key driver for the creation of this policy. What is it?

   The "Considerations for Cloud Computing Services" section identifies one risk of using the cloud. What are three other risks of using cloud computing?

4) **Language of Policy:**
   In the table describing the different levels of data (that is, Level A, B, C, D), the "Cloud Use" column uses various words like "can," "cannot," "should," and "may." Why does the author use these words in these cases?

5) **Policy Structure:**
   What items are missing from the policy footer?

Cloud Computing Policy Debrief

Note that this section contains a debrief and potential lab answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after the group discussions have taken place.

Define Scope

All PharmaCo employees including, but not limited to, staff, scientists, researchers, contractors, and individuals who procure or utilize cloud computing services.

All cloud computing resources that provide storage services involving the processing, exchange, storage, or management of corporate data.

The "Scope" section in the draft policy refers to "All PharmaCo employees." This is very comprehensive, but it can be improved in two ways:

1) **Fully define constituents.**
   By explicitly defining the people to whom this policy applies, you can make it more personal and a little more obvious to whom it applies. In case you have left anyone out, the clause "but not limited to" is also included. Even better, you refine the scope to include anyone who procures or utilizes cloud services.

2) **Define technology.**
   In addition to people, it is also important to define the scope of services to which this policy applies. By defining the scope to include essentially any cloud services (for example services, platforms, and infrastructure that process, exchange, or store data) that deal with corporate data, you have very specifically defined the scope so it is clear to readers.

General or Specific and Why?

Cloud storage services are provided by companies such as **Box, Dropbox, Google (Drive), and Microsoft (OneDrive)**. These cloud computing services are generally easy for people and organizations to use, they are accessible over the internet through a variety of platforms, and they may be able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

The "Overview" section does a nice job describing the context of this policy. However, one sentence mentions certain companies by name. This is somewhat unusual for a high-level policy. Why did the author mention Box, Dropbox, Google, and Microsoft in this policy draft?

Based on your research within PharmaCo, you know that people are already using cloud services. It will likely be difficult to get them to change. There will be resistance. By mentioning these companies, you are acknowledging, in some small way, that you know the cloud services provided by these companies exist and are valuable. You are giving a nod to your users, who may have a strong positive feeling about these services. Given that PharmaCo has a history and culture of decentralized operations and decision making, you are making the policy a bit friendlier and inviting to read.

Identify Risks

Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Risks with using self-provisioned cloud services include:

- Unclear, and potentially poor access control or general security provisions
- Sudden loss of service or data without notification
- Data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy
- The exclusive intellectual rights to the data stored, processed, or shared on cloud service may become compromised.

Your research within PharmaCo identified that various business units were procuring their own cloud services without any central management or oversight. You can't stop all of this activity overnight, but you can take a step to better protect the company's most sensitive assets. This is why the policy states, "Employees may not self-provision cloud services to store, process, share, or manage Level A: Regulated Data." Mapping the policy to the company's overall data classification is a good move that enables you to clearly define the cases in which employees cannot self-provision their own cloud services.

These self-provisioned cloud services introduce other risks to the organization. The "Considerations for Cloud Computing Services" section lists just one risk: "Unclear and potentially poor access control or general security provisions." Explicitly defining other risks, as shown above, also help readers understand why these services are not appropriate, especially for "Regulated Data."

Language of Policy

Level A: Regulated Data

Must not use self-provisioned cloud services to store, process, share, or otherwise manage regulated institutional data.

Level B: Confidential Data

Should not use self-provisioned cloud services to store, process, share, or otherwise manage confidential data without ensuring that a service's safeguards are appropriate for confidential data.

The language used in the draft policy document indicates that it was carefully thought out. Because use of self-provisioned cloud services cannot be stopped or even managed all at once, this policy takes a reasonable, risk-based approach.

For the most sensitive "Regulated Data," self-provisioned cloud services are not allowed. Period.

For less sensitive data, such as "Confidential" or "Administrative," self-provisioned cloud services "should not" be used. Guidance is also provided to say that users "should" use centrally or locally provisioned cloud services.

For "Public" data, self-provisioned cloud services "may" be used.

Policy Structure

Approval Date:
January 11, 2022

Effective Date:
January 11, 2022

Review Committee:
Information Risk Steering Committee
IT Executive Council

Responsible Departments:
Information Technology, Information Security, Finance

Review Cycle:
Annually or as required by relevant external regulation.

Finally, the policy should also include standard elements including the approval date, effective date, responsible departments, and the review cycle.

Policy Assessment

- When assessing policy, consider these key questions:
  - Is this policy fragment clear and concise?
  - Does it meet SMART objectives?
  - Does it outline responsibility and compliance?
  - Does it designate required actions?
  - Does it provide sufficient guidance from which a specific procedure can be developed?

The policy statement, or body of the policy, identifies the actual guiding principles or what is to be done. The statement is designed to influence and determine decisions and actions within the scope of coverage. The statement should define actions that are prudent, expedient, or advantageous to the organization. When you are reviewing policy, it should state what is supposed to be done and who is supposed to do it.

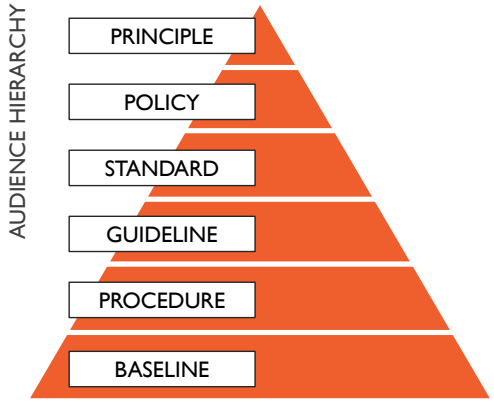
Note: Policy is not detailed; it does not have step-by-step information. That is done with procedures. The rule of policy assessment is that it is enough information to point to the appropriate procedure. In general, procedures can be updated with far less review than policy.

Summary

This page intentionally left blank.

Purpose of Policy

- Protect people
  - Safety from discipline if following policy and procedure
  - Establish the bounds of acceptable behavior
  - Empower people to do the right thing
- Protect the organization
  - Ensure data and systems are protected
  - Comply with regulations and laws



Policy Protects People
Organizations should adopt an umbrella policy so that to the extent possible, people should be able to work without fear. They should know that as long as they are following the policy, they are safe if something bad should happen. However, there is no substitute for the brain. They should also know that they are expected to use common sense.

One of the most important characteristics of policy is to establish bounds for behavior. Organizations typically have policies on a variety of subjects. What policies does your organization have that specifically relate to security? Identify what your organization does or does not have, and try to make it better. Your actions may include lobbying to create or expand current policy. Without a security policy, any organization can be left exposed to the world. To determine your policy needs, you must first conduct a risk assessment. This may require an organization to define levels of sensitivity with regard to information, processes, procedures, and systems.

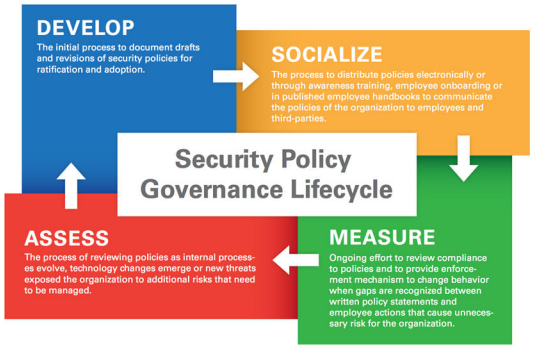
Policy Protects the Organization
Safeguarding information is a challenge when records are created and stored on computers. We live in a world where computers are globally linked and accessible, making digitized information especially vulnerable to theft, manipulation, and destruction. Security breaches are inevitable. Crucial decisions and defensive action must be prompt and precise.

A security policy establishes what you must do to protect information stored on computers. A well-written policy contains sufficient definition of "what" to do so you can identify and measure or evaluate the "how."

An effective security policy will help protect the company from legal and financial actions; however, it also has the effect of protecting people. Anyone who makes decisions or takes action in a situation in which information is at risk incurs personal risk also. A security policy allows people to take necessary actions without fear of retaliation.

Tips for Creating Successful Policy

- Align policy with your organization's security posture or culture
  - Use language appropriately
  - Favor positive voicing when possible ("always do" versus "never do")
  - Short and clear policy is ideal
- Adopt a life cycle approach
  - Security policy will change with business
  - There is no "perfect" policy
  - Improve policy over time as capabilities mature



You now have a framework for evaluating policy. When you get back to your organization, we hope that you will put what you have learned into practice! Take the steps in order, and the framework will work for you. Revisit your mission statement and ask questions to see if your organization is living up to its mission. Start with a corporate policy. Ensure you have the support of senior leadership and help them state that good security is good business in a manner that cannot be misunderstood. Make sure you have the required policies and that they have the required elements written in a clear, concise manner.

Use a naive (not familiar with this exact topic), detail-oriented person to help you assess the specificity of the policy. Someone familiar with the topic might "autocorrect" or "mentally fill in" any errors or omissions. If you wrote the policy, employ someone who knows the organization and fundamentals of information security to review the content. Remember that the threat level can change, and policy should be reviewed in light of major changes.

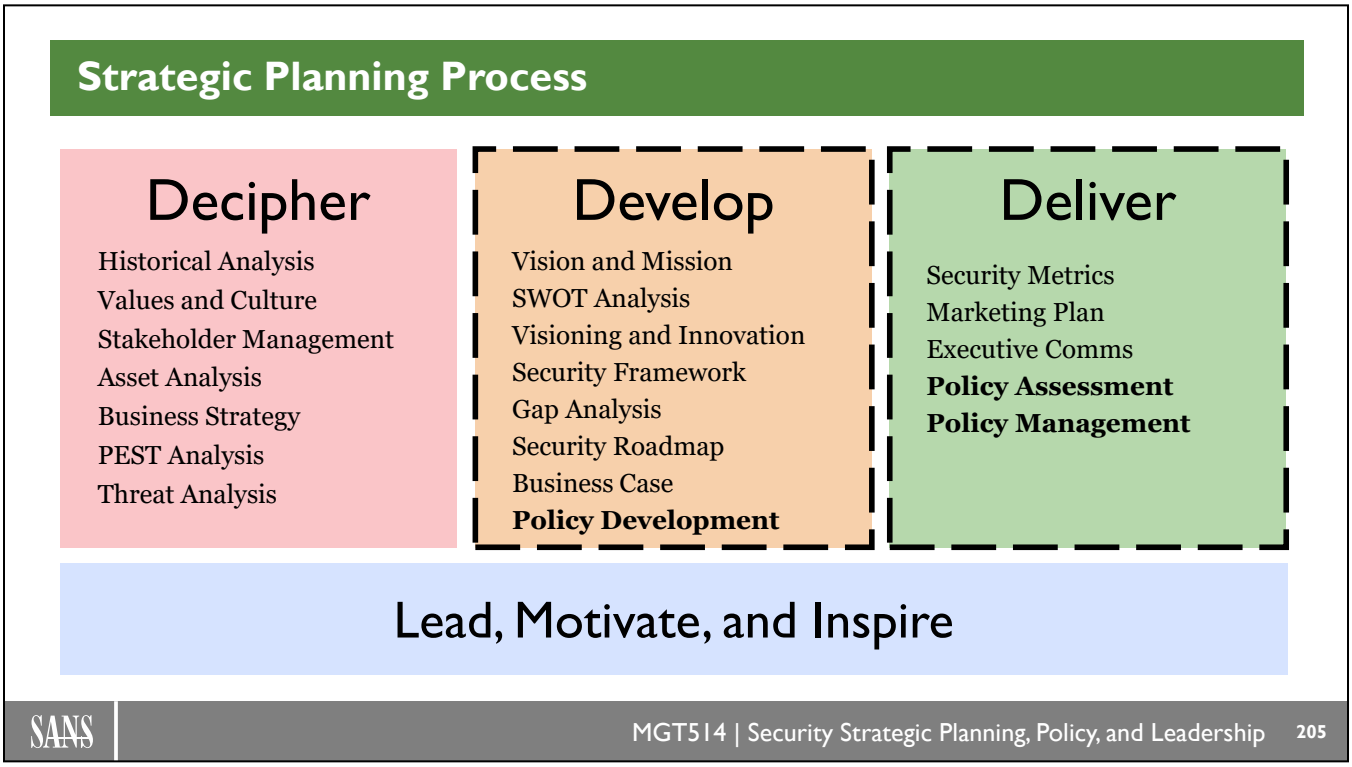
Course Roadmap

- Section 1: Strategic Planning Foundations
- Section 2: Strategic Roadmap Development
- ***Section 3: Security Policy Development & Assessment***
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 3

- Purpose of Policy
  - Policy Pyramid
- Develop Policy
  - Language of Policy
    - Lab #1: Positive and Negative Voicing
  - Policy Structure
  - Policy and Culture
  - Define Requirements
  - Development Examples
    - Lab #2: Vulnerability Management Policy
- Manage Policy
  - Approve, Socialize, and Measure
- Assess Policy and Procedure
  - SMART Approach
  - Policy Assessment
    - Lab #3: Cloud Computing Policy

This page intentionally left blank.



In this section, we focused on the Develop and Deliver phases of strategic planning with a discussion on policy development, management, and assessment.