SEC301 | INTRODUCTION TO CYBER SECURITY
GIAC Information Security Fundamentals (GISF)

301.1

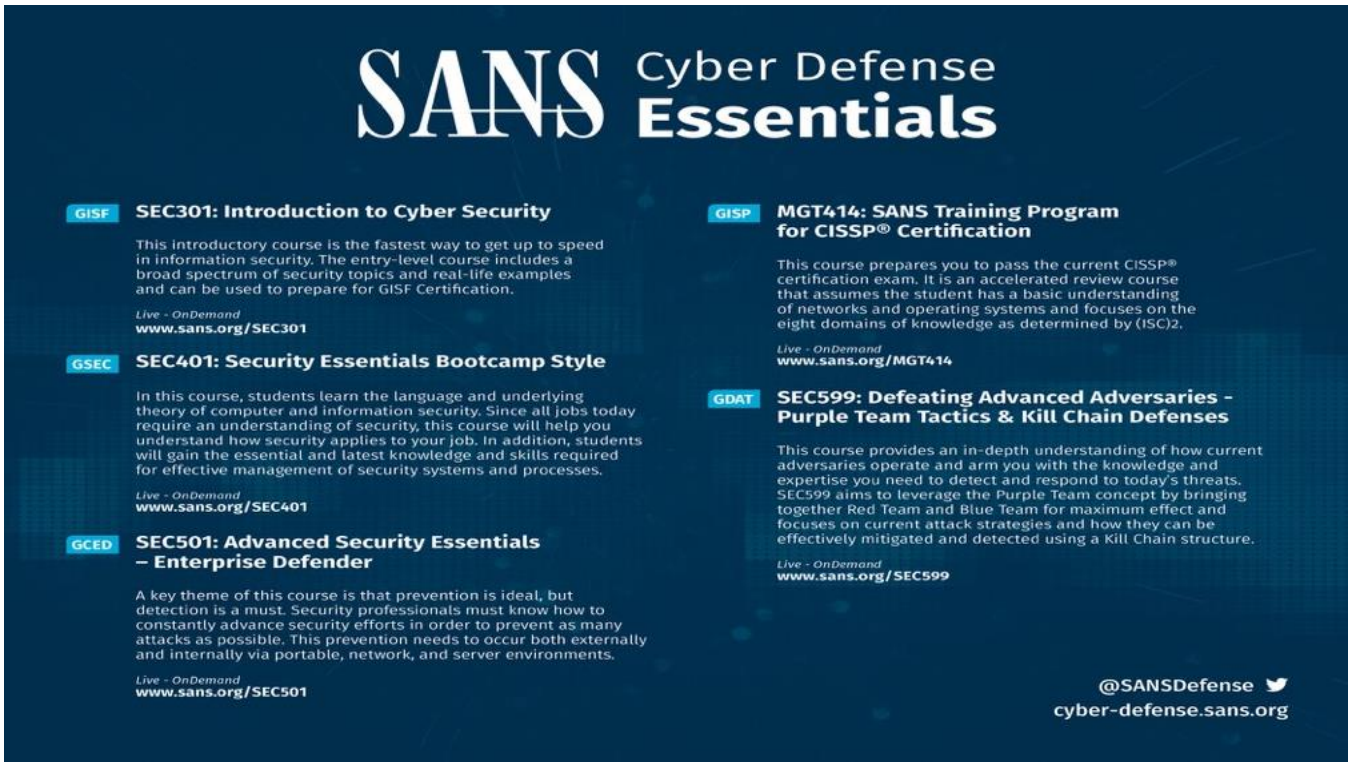
Security's Foundation

SEC301.1 | Introduction to Cyber Security

SANS

Security's Foundation

This page intentionally left blank.



This page intentionally left blank.

SANS Cyber Defense Essentials

GISF **SEC301: Introduction to Cyber Security**

This introductory course is the fastest way to get up to speed in information security. The entry-level course includes a broad spectrum of security topics and real-life examples and can be used to prepare for GISF Certification.

Live - OnDemand
www.sans.org/SEC301

GSEC **SEC401: Security Essentials Bootcamp Style**

In this course, students learn the language and underlying theory of computer and information security. Since all jobs today require an understanding of security, this course will help you understand how security applies to your job. In addition, students will gain the essential and latest knowledge and skills required for effective management of security systems and processes.

Live - OnDemand
www.sans.org/SEC401

GCED **SEC501: Advanced Security Essentials – Enterprise Defender**

A key theme of this course is that prevention is ideal, but detection is a must. Security professionals must know how to constantly advance security efforts in order to prevent as many attacks as possible. This prevention needs to occur both externally and internally via portable, network, and server environments.

Live - OnDemand
www.sans.org/SEC501

GISP **MGT414: SANS Training Program for CISSP® Certification**

This course prepares you to pass the current CISSP® certification exam. It is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses on the eight domains of knowledge as determined by (ISC)2.

Live - OnDemand
www.sans.org/MGT414

GDAT **SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses**

This course provides an in-depth understanding of how current adversaries operate and arm you with the knowledge and expertise you need to detect and respond to today's threats. SEC599 aims to leverage the Purple Team concept by bringing together Red Team and Blue Team for maximum effect and focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure.

Live - OnDemand
www.sans.org/SEC599

@SANSDefense
cyber-defense.sans.org

Course Outline (1)

- Day 1: Security's Cornerstone:
  - Core Principles
    - Lab 1.1: Introduction to the Lab On Demand System (LODS) and Quizzes
  - Risk Management
  - Security Policy
  - Authentication, Authorization, and Accountability
    - Lab 1.2: Building Better Passwords: The Haystack

This will be our least technical day.

This page intentionally left blank.

Course Outline (2)

- Day 2: Computer Function and Networking:
  - How Computers Work
    - Decimal/Binary/Hex Numbers/ASCII/RAM vs HDD
    - Lab 2.1: Converting Number Systems
  - Networking 101 and 102
    - Lab 2.2: Networking

- Day 3: An Introduction to Cryptography
  - Intro to Crypto
    - Lab 3.1: Crypto by Hand
  - Building Blocks of Modern Crypto
    - Lab 3.2: Visual Crypto
  - Data Encrypting Protocols

This page intentionally left blank.

5 Days — 9 Labs (two per day except Day 5) — Estimated hands-on time: 5+ hours

Course Outline (3)

- Day 4: Cyber Security Technologies, Part 1
  - Wireless Security & IoT
    - Lab 4.1: Wireless Access Point Configuration
  - Network Attacks
  - Malware and Anti-malware
    - Lab 4.2: Anti-malware Scanning, Malware Bytes
- Day 5: Cyber Security Technologies, Part 2
  - Network Security Technologies (compartmentalization / firewalls / IDS-IPS sniffers / content filters / and so on ...)
    - Lab 5.1: Firewall Builder
  - Browser and Web Security
  - System Security (hardening, patching, virtual machines, cloud, backup)

This page intentionally left blank.

Module Review Questions & SEC301.com

- After the lecture slides in each day's book…
  - You will find Module Review Questions
  - Behind the review questions are the answers
- Plus – http://www.sec301.com – Quizzes, videos, and more
  - Username: student
  - Password: asimplepassword

Module Review Questions & SEC301.com

At the end of each day's book, just after the final lecture slide, you will find a series of review questions for each module. Behind those, you will find the answers to those review questions. Depending on time, these may or may not be covered in class. In any case, you have them available.

Another resource you should be aware of is the course website. The website is available on the internet not just while you are in class, but anytime day or night following class. Here you will find access to module quizzes (different from those in the back of the books), videos of the author performing and explaining the labs, and additional information to benefit you. To access the site, simply go to:

http://www.sec301.com
Username: student
Password: asimplepassword

Warning! Acronyms Ahead

- If you work in or around IT (Information Technology) …
- … you will hear a lot of acronyms!

- In SEC301, you will learn acronyms and become used to hearing them

Warning! Acronyms Ahead

It is a simple fact that Information Technology (IT) workers use an astounding number of acronyms when speaking to each other. If you are going to work in or around IT, you have to get used to hearing them, recognize them for what they are, and understand as many of them as possible.

For this reason, one of the goals of the SEC301 course is to get you used to hearing acronyms. Another goal is to teach you the meanings of the more common acronyms used in IT.

One of the most important things the Introduction to Cyber Security course strives to do is get you used to a lot of new terminologies, which happens to include a great number of TLAs (Three-Letter Acronyms).

GIAC – The GISF Test

- Many SANS classes have a GIAC certification attached
  - GIAC = Global Information Assurance Certification
  - For SEC301, the cert is the GIAC Information Security Fundamentals (GISF)
  - For the latest updates on this certification, see: https://www.giac.org/certification/information-security-fundamentals-gisf
- Currently for GISF Specifically:
  - 1 proctored test (given at Vue Testing Centers)
  - 75 Questions
  - 2 hour time limit
  - 72% to pass (subject to change)
  - Tests are open book / open note

GIAC – The GISF Test

Many of the classes taught by SANS have a certification attached to them. For example, the GISF certification is attached to SEC301 – meaning that all the information needed to pass that certification test is in the SEC301 course books. SEC401 has the GSEC certification, SEC501 has the GCED certification, etc.

Currently (as of September 2022), GISF consists of one proctored test given at Vue Testing Centers. The test is 75 questions and has a 2-hour time limit. A passing score of 72% is required, though that percentage does change occasionally.

Note that all GIAC certification tests are open book and open note. Any printed material is allowed into the testing room with you. While it is good that you can look up answers, it also means that any fact in those books is fair game on the test. You will want to build an index of topics, their page number, and their book number so you can look things up quickly. Be warned – you will NOT have enough time on the test to look up all of the answers. Using the index wisely will bump your score about 10 percentage points, hopefully getting to a passing score. The author does not provide an index for a simple reason. Creating the index requires you to read through the books at least once. Reading the books raises your odds of passing the test.

GIAC Certification Questions

- How GIAC Certification tests work
  - Professional question writers create the questions from the contents of the course books and the lab workbook
  - All questions are supported by the courseware material
    - But they are not verbatim from the courseware
  - The knowledge to answer the questions is in the courseware
  - All questions are single-answer multiple choice
  - Example: If the course explains how to do Binary/Hex conversions
    - You might be asked to do that on the test
    - The knowledge of how to do that is in the course book or in the lab guide
    - However, the example in the book and the example on the test will be different

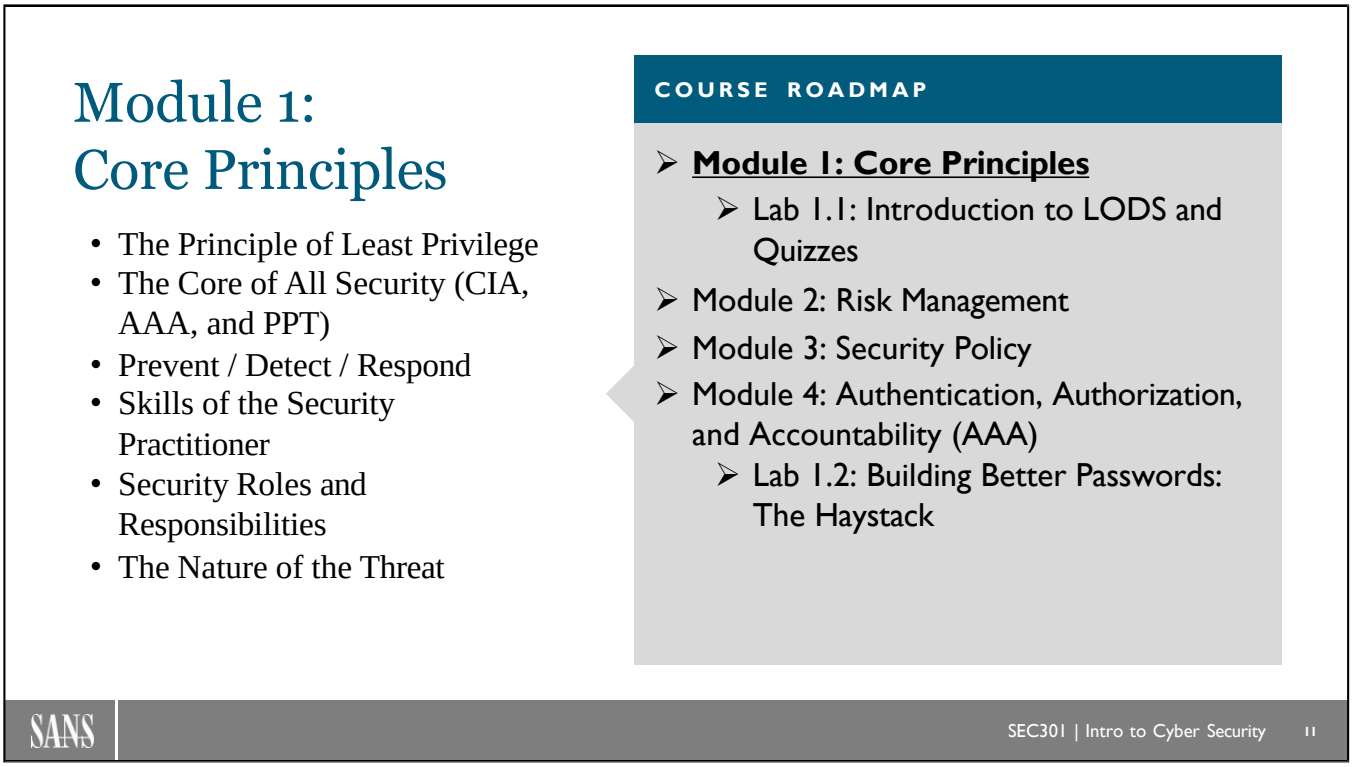
GIAC Certification Questions

All GIAC certification questions are written by professional question writers. These writers go through the books, see something they could write a question about, and write that question. In other words, all of the questions on the certification test come from inside the books you are issued for your class. The books used to create questions are all of the "daily books" lectured in class as well as the lab-guide. Be aware, the version of the test you will take is tied to the version of books you received.

Note that while all questions come from the courseware, they are not taken verbatim from the courseware. The knowledge to answer the question is in the book, but not the specific answer.

For example: Later in the course, we will cover converting binary and hexadecimal values. You may very well be asked to do that on the test. However, the example on the test and the example in the book will not be the same. You will have to know how to do that conversion (and yes, an on-screen calculator is available). ☺

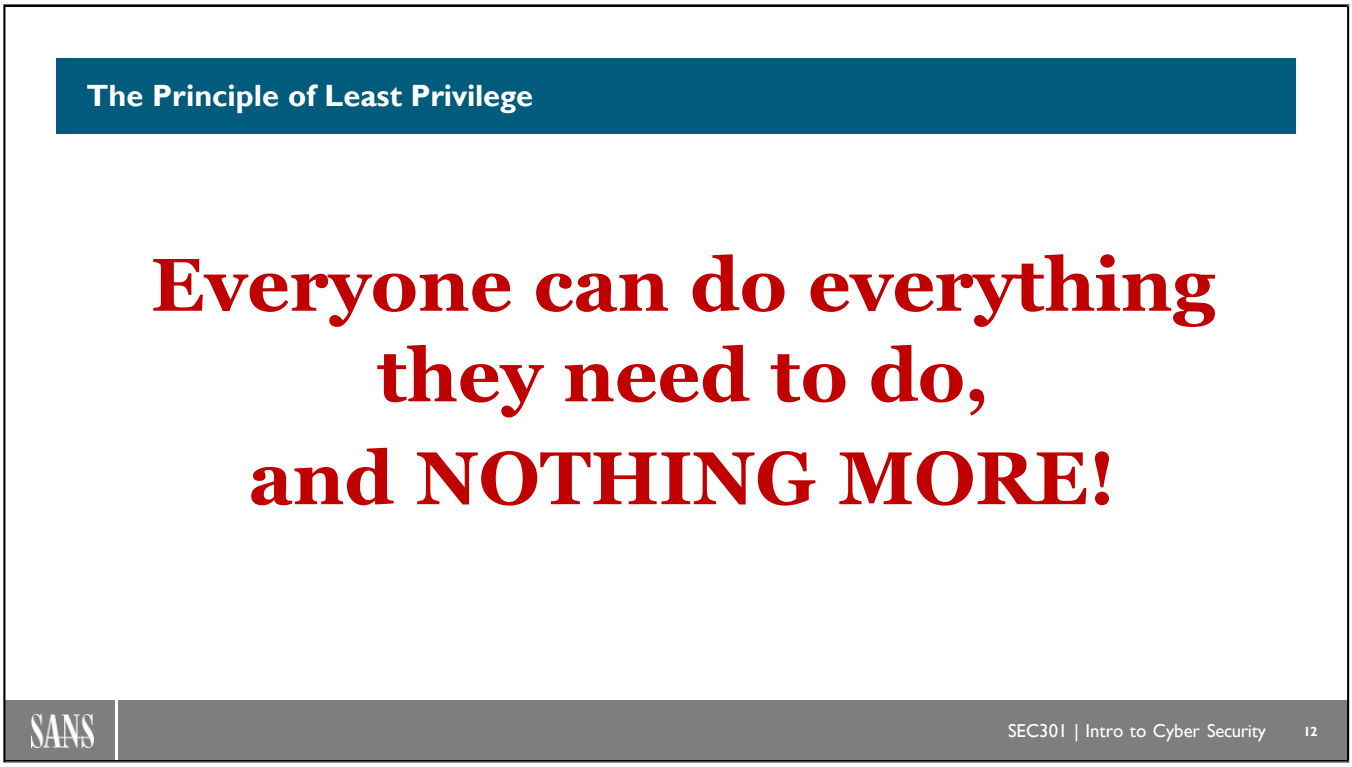
Every GIAC certification test question is a multiple choice question with a single correct answer. There are no "choose two" questions, no "all of the above" questions, and no "true/false" questions.



Module 1: Core Principles

In this section, we cover the following:

- The Principle of Least Privilege
- The Core of All Security (CIA, AAA, PPT)
- Prevent / Detect / Respond
- Security by Thirds
- Security Roles and Responsibilities
- The Number 1 Goal of Security
- The Nature of the Threat



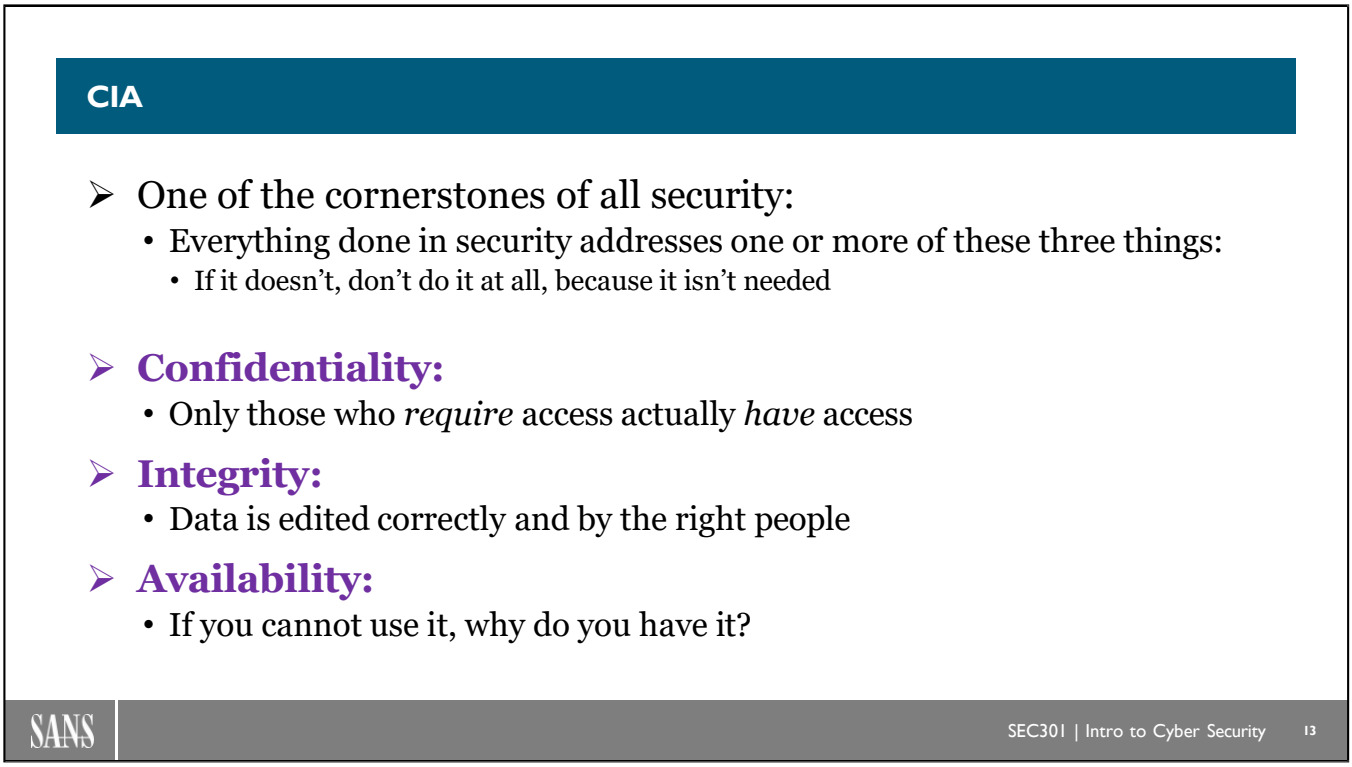
The Principle of Least Privilege

This is one of the most important, if not ***the*** most important, lessons of this course. In order to do security well, you have to get to the point where the principle is instinctual. You don't think about implementing Least Privilege—you just do it, and you do it correctly.

There are two common mistakes made in the implementation of the Principle of Least Privilege:

1. The security team is too restrictive with its rules and settings. When security gets in the way of the mission or the organization, security is wrong, not the mission.
2. The last three words ("and nothing more") are often left out of the principle. The examples are, unfortunately, numerous. We give users all the access they need and a lot more. This typically occurs because it is easy. If everyone can access everything, we don't have to worry about managing access.

Done correctly, users should be given only the access and capability they need to do their jobs and nothing more than that.



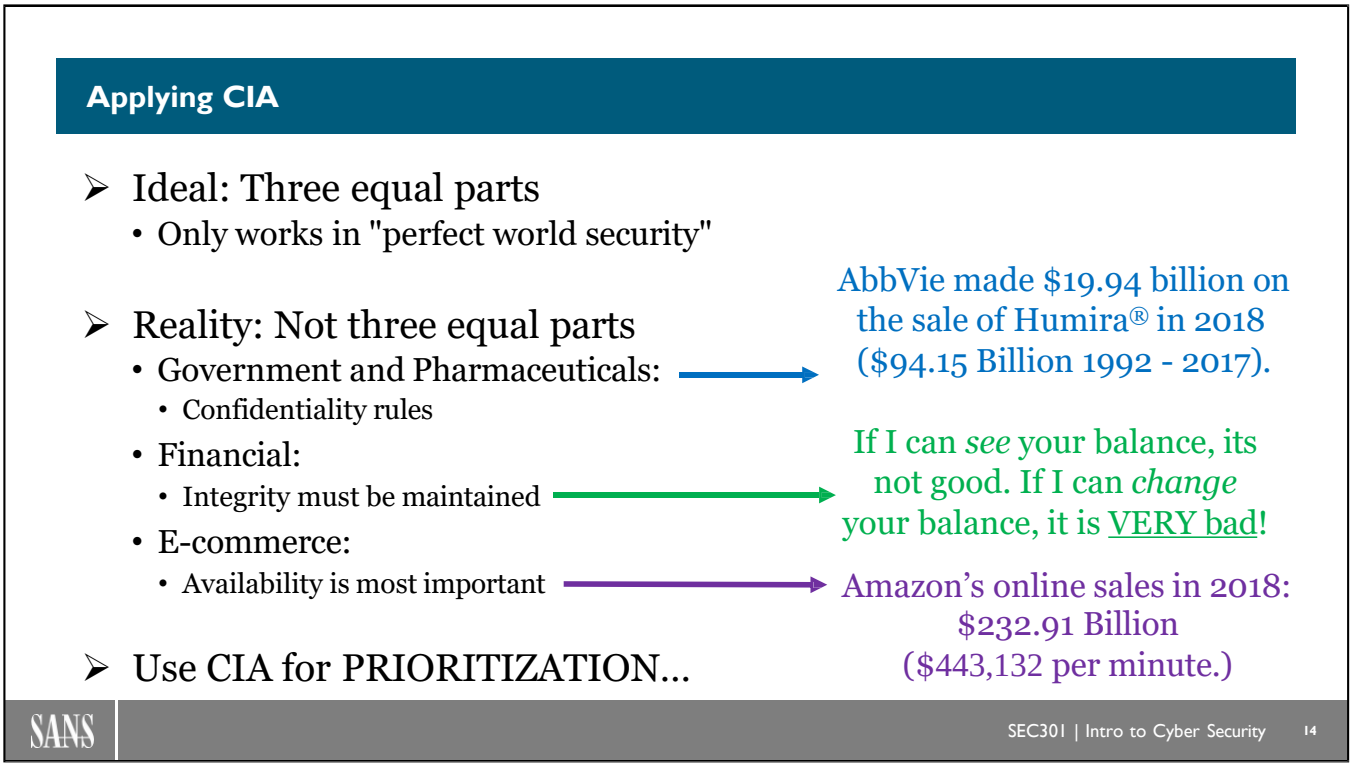
CIA

CIA is the cornerstone of all security. Everything we do as security practitioners addresses one or more of the components of CIA. If you are doing things in your security program that do not address one of these, you are doing the wrong stuff.

The principles behind CIA are straightforward:

- **Confidentiality:** Only those who need access to something have access to it. The confidentiality of information is protected.
- **Integrity:** Data should be modified only by the correct people, in the correct way, and with the correct information.
- **Availability:** If you are unable to use it, why do you have it? Whether it be a piece of data, a server, or any other resource, it has to be available when we need it, or it does us no good.

This is sometimes referred to as the CIA triad since ideally, you address all three of these in equal measure. After all, the definition of *triad* is three equal parts. However, that does not always happen, and sometimes you can make a valid case for giving added weight to one of these three pieces.



Applying CIA

As stated, in a perfect world, every organization would give equal weight to each of the three pieces of the CIA. However, certain industry sectors will give added attention to one of these.

For example, in the pharmaceuticals industry, **confidentiality** is absolutely vital. Other companies could make a particular medicine if they had the exact formula. To give you an idea of just how valuable a formula for medication can be, note that in 2017, AbbVie made almost $18.43 billion on the sale of Humira® in that year alone. Granted, Humira® is considered the most valuable drug formula patent in history, so not all drugs manage those lofty numbers. Still, protecting a formula of that nature, especially while it is still in development and is not yet fully patentable is of vital importance.

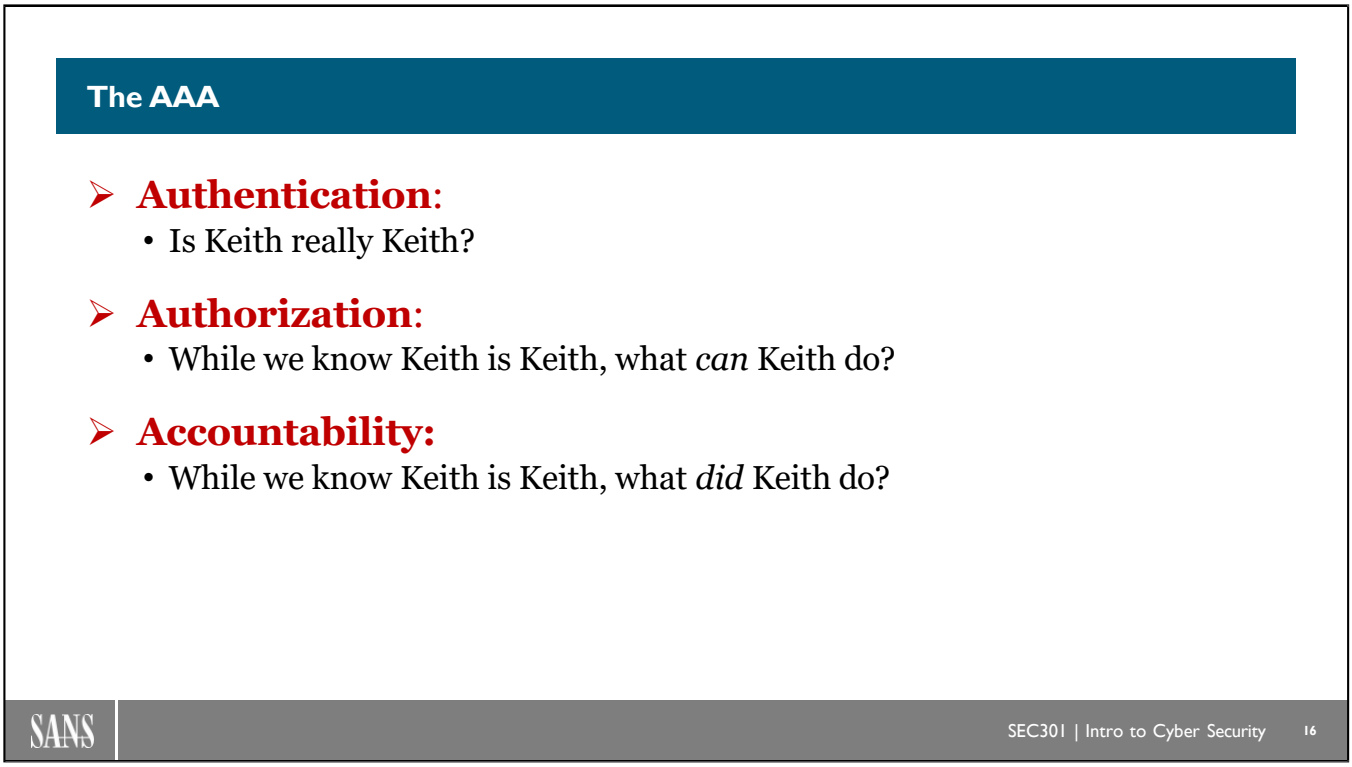
In the financial sector, **integrity** is most important. If you think you have a million dollars in your bank account and the bank tells you your balance is $1.27, you will probably not be happy.

In the e-commerce sector, **availability** absolutely rules. Online sales have become important for the stores that have brick-and-mortar outlets such as Walmart, Sam's Club, Target, and Costco. however, when you look at a company like Amazon where there are few physical stores, availability of the company's website must be absolute. Again, what is the potential monetary impact? In 2018, *one minute of downtime* for the Amazon.com website would have cost the company $443,132 in revenue. (That is up from just $338,242 per minute in 2017).

As you can see, each of these sectors legitimately gives more consideration to one piece of CIA than another. Understand, though, that all of these sectors care about all three components. As just one example, one of the ways a bank protects the integrity of your bank account is by not letting other people log into your online bank account. Strong authentication measures are usually thought of as confidentiality measures, and they are, but here the bank uses them primarily to protect integrity. If you cannot log into your online bank for a while, it is inconvenient, but certainly not as big an issue as a modified balance.

The chart below depicts this impact of Distributed Denial of Service (DDoS) against Amazon.com over each of the last several years. The revenue is broken out by year, month, week, day, hour, minute, and second. DDoS is much more than a simple nuisance to a company like Amazon.

	2013	2014	2015	2016	2017	2018
Revenue in $B	$74.45	$88.98	$107	$135.98	$177.78	$232.91
Year	$74,452,000,000	$88,988,000,000	$107,006,000,000	$135,987,000,000	$177,780,000,000	$232,910,000,000
Month	$6,204,333,333	$7,415,666,667	$8,917,166,667	$11,332,250,000	$14,815,000,000	$19,409,166,667
Week	$1,431,769,231	$1,711,307,692	$2,057,807,692	$2,615,134,615	$3,418,846,154	$4,479,038,462
Day	$203,978,082	$243,802,740	$293,167,123	$372,567,123	$487,068,493	$638,109,589
Hour	$8,499,087	$10,158,447	$12,215,297	$15,523,630	$20,294,521	$26,587,900
Minute	$141,651	$169,307	$203,588	$258,727	$338,242	$443,132
Second	$2,361	$2,822	$3,393	$4,312	$5,637	$7,386

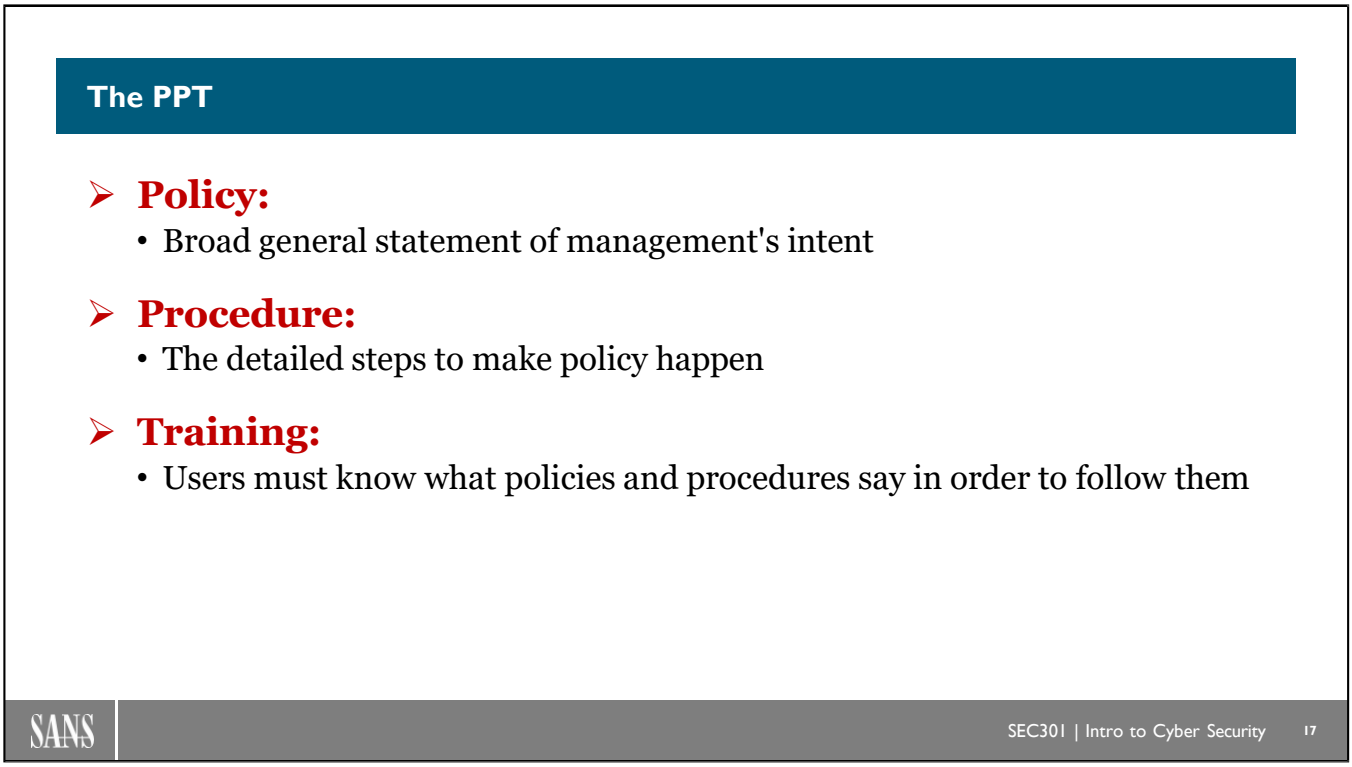


The AAA

We have an extensive module devoted to the topic of AAA later in the course. For now, we simply introduce it as a concept.

AAA is another one of the vital pillars of a good security program. The better you implement these three pieces, the more secure your organization will be:

- **Authentication**: Authentication is the process of verifying someone's identity. Is the user who claims to be Keith really Keith? We force that user to authenticate so that we know for certain he is who he says he is.
- **Authorization**: Once we know that Keith really is Keith, what are we going to let Keith do? Which files will we allow him to access? Which servers can he utilize? What resources are available to him?
- **Accountability**: Although we know that the user Keith is really Keith, what exactly did Keith do? Did he attempt unauthorized access to files, servers, or other resources? Did he try to visit inappropriate websites? Or, was he a "good boy" and just did his job?

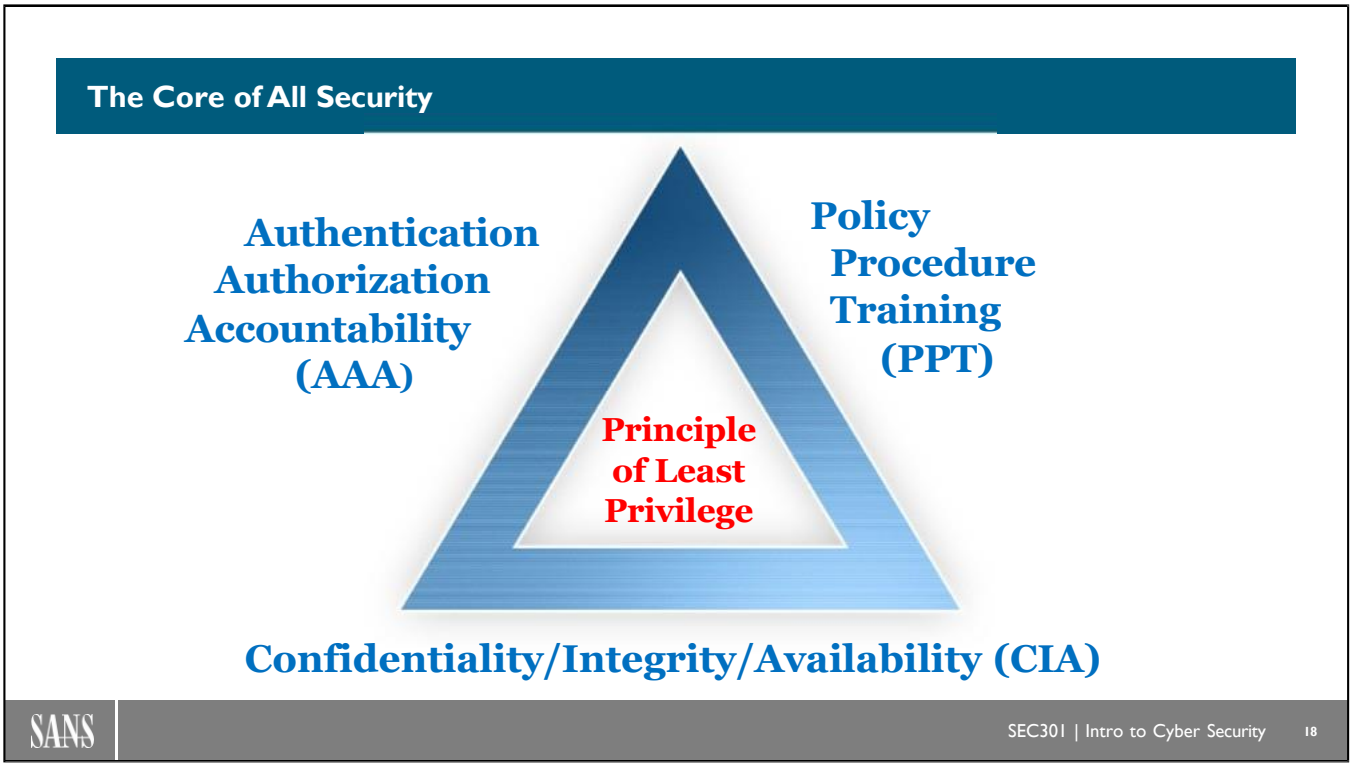


The PPT

We also have Policy, Procedure, and Training. Simply stated, if you do not have these three things in place, you do not have a security program, or, you likely don't have a program that has any possibility of being effective. Following are descriptions of the components of the PPT:

- **Policy:** A policy is a broad general statement of management's intent. It is a legal document that spells out the general sense of how management expects the assets of the organization to be protected.
- **Procedures:** Procedures are the detailed steps that dictate precisely how policy should be put into place. They describe the step-by-step procedures to implement the broad general statement of management's intent (the policy).
- **Training:** Training is how everyone knows what the policies and procedures say. You can create the best policies and procedures in the world but not tell anyone what they say ... this does you no good. You can't very well expect anyone to follow those policies and procedures if they don't know they exist. You also cannot get upset with your users for not following them, and you certainly cannot take disciplinary action against them.

At this point, we simply introduce the concept of the PPT. We go into more detail in later sections of the course.



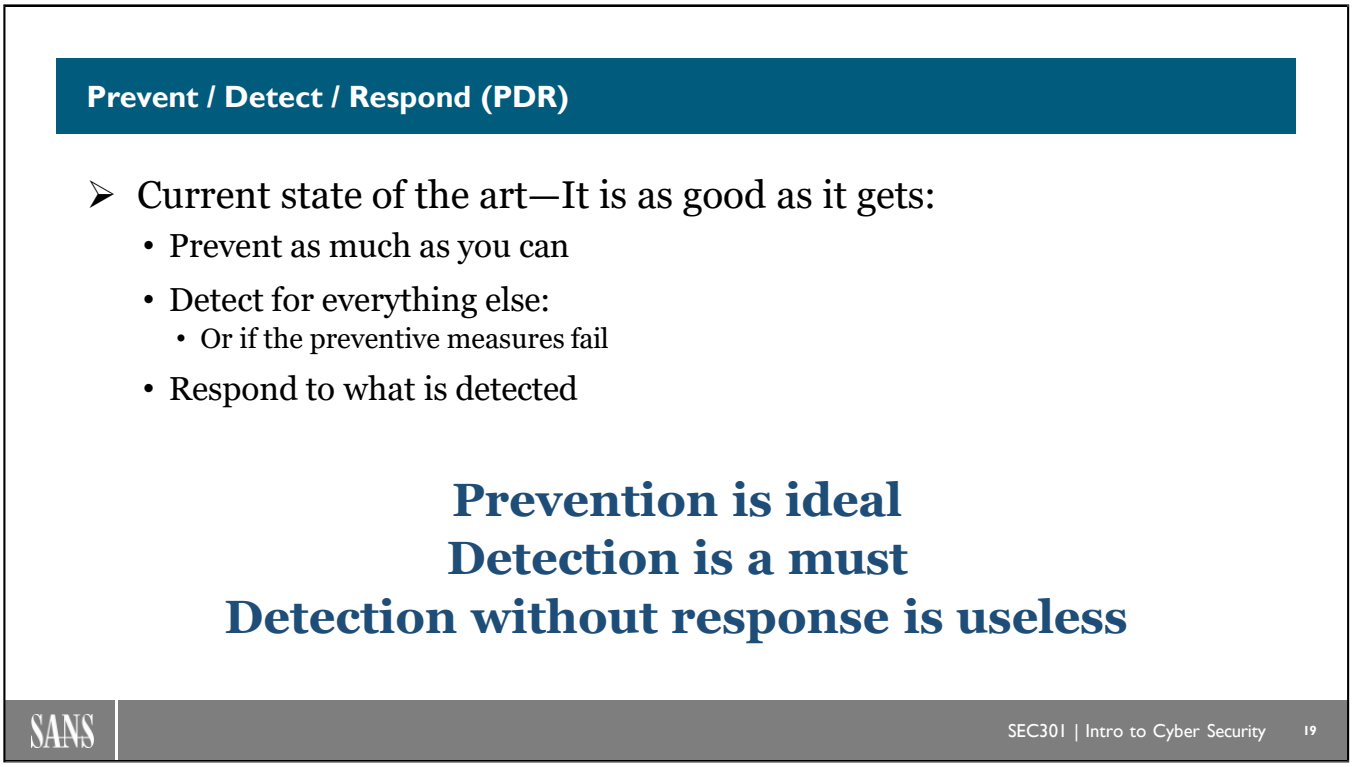
The Core of All Security

Nothing we have talked about to this point stands alone. The CIA is the cornerstone of all security and absolutely vital; however, it needs help to be effective. That help comes from a myriad of places.

Achieving Confidentiality, Integrity, and Availability (CIA) requires the good implementation of Authentication, Authorization, and Accountability (AAA). You will not have effective AAA without solid Policy, Procedure, and Training (PPT).

All of this supports the fundamental security goal of the *Principle of Least Privilege:* Everyone can do everything they need to do, and nothing more.

Keep this fundamental concept in mind about security: Nothing in security stands alone. Here, you see four critical elements tied together in a nice neat package. But even this is not the whole story. In addition to the very important items we have discussed, a security program needs all of the elements we will discuss throughout this course—physical security, risk management, incident response, and so on. All of it interweaves to form the security posture of an organization. You cannot look at any one piece to get the complete picture.



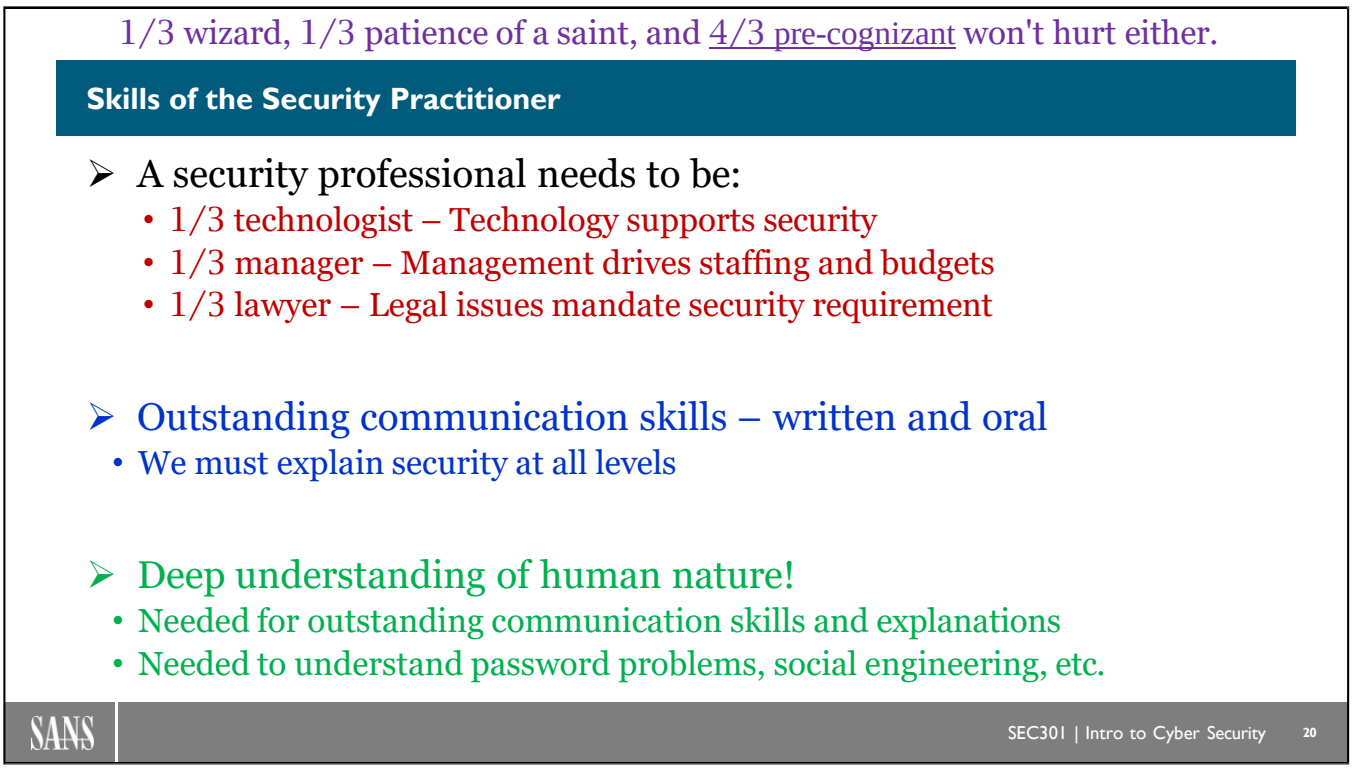
Prevent / Detect / Respond (PDR)

The current state of the art in security can be summed up as Prevent / Detect / Respond. In other words, you *prevent* as much of the bad stuff as you possibly can. You *detect* for anything you can't prevent (or if your prevention fails). You *respond* whenever detection occurs.

Here are other core themes of this course:

- Prevention is ideal.
- Detection is a must.
- Detection without response is useless.

The first method (PDR) expresses the exact same idea. You will see this concept (PDR) repeatedly throughout the remainder of the class. (From here on, we will use the second way to express the concept when needed: Prevention is ideal. Detection is a must. Detection without response is useless.)



Skills of the Security Practitioner

When you truly look at the security field and the skill sets required by the security practitioner, the job does not involve a single set of skills. Perhaps the best you will ever hear this summed up is:

A good security practitioner is:

- 1/3 technologist
- 1/3 manager
- 1/3 lawyer

People who can claim expertise in all three areas are rare and valuable. In other words, the security professional who can do all the following is a rare person and exactly what every security professional should aspire to be:

- Walk into the IT system administrator's shop and explain security so that they understand.
- Walk into the board of directors' meeting and talk about security so that the directors understand.
- Then, walk into corporate legal and talk to the lawyers about security in terms they understand.

Do you notice that everything above, and so much more, requires outstanding communications skills. We must develop both writing and oral communications skills that allow us to explain security to everyone in the organization from the Senior Manager on down.

You cannot develop outstanding communications skills unless you have a deep understanding of human nature. It is required to speak and/or write words that move and motivate people.

Understanding human nature is also necessary in so many other aspects of Cyber Security. For a simple example, take passwords. Getting the technical aspects of passwords right is not terribly difficult – just choose and properly implement the correct technologies. Getting the human nature aspect of passwords right is much more difficult. It is the human that chooses the password in most cases and where the failing comes far more frequently than in the technology.

Note that we are making a bit of a joke here as well with the comment regarding "1/3 wizard, 1/3 pre-cognizant, and 4/3 the patience of a saint." Although there is indeed an attempt at humor, there is also a serious vein as well:

- Management often expects the equivalent of wizardry from the security staff.
- Many of a security practitioner's duties require pre-cognizance (determining the likelihood of threat requires predicting the future).
- We often need to exercise great patience when dealing with management and users who just don't want to believe our security measures are necessary.

Roles and Responsibilities (1)

- Senior Manager:
  - Has legal responsibility to protect the assets of the organization
    - That gives them the ultimate responsibility for security
  - Authority can be delegated—responsibility cannot be
  - Senior Manager means:
    - Commercial (.com) = CEO
    - DoD (.mil) = Commander
    - Government (.gov) = Director, Secretary, and such

Roles and Responsibilities (1)

There are certain roles in any organization that you want to be aware of. Each of these roles has a particular set of responsibilities with regard to your security program.

The first role we discuss is the Senior Manager. That term has a different meaning in different industry sectors. In the commercial (.com) world, that role has the title of CEO. In the DoD (.mil) arena, that role has the title of Commander. In the government (.gov) sector, the title is Director, Secretary, or whatever title is assigned to the head of that government agency.

By whatever title, the Senior Manager has the legal responsibility to protect the assets of the organization. Because the security program is all about protecting assets, this means that they also have the ultimate responsibility for security.

For example, later we discuss *risk decisions*. One of those decisions is to "accept risk." It is not the security practitioner's job to make the risk decision. It is the Senior Manager's job to do that. We advise, consult, and recommend. But it is their legal (and sometimes moral) responsibility to make the final decision.

Remember, they can delegate the authority to implement security to the Chief Information Security Officer, but the responsibility rests on the Senior Manager's shoulders.

Roles and Responsibilities (2)

- Data Owner:
  - Person with primary responsibility for data
  - Owners determine classification, protective measures, and more
- Data Custodian:
  - The person/group that makes the decisions of the owners happen
- Users:
  - Use data
  - Are also automatically Data Custodian s

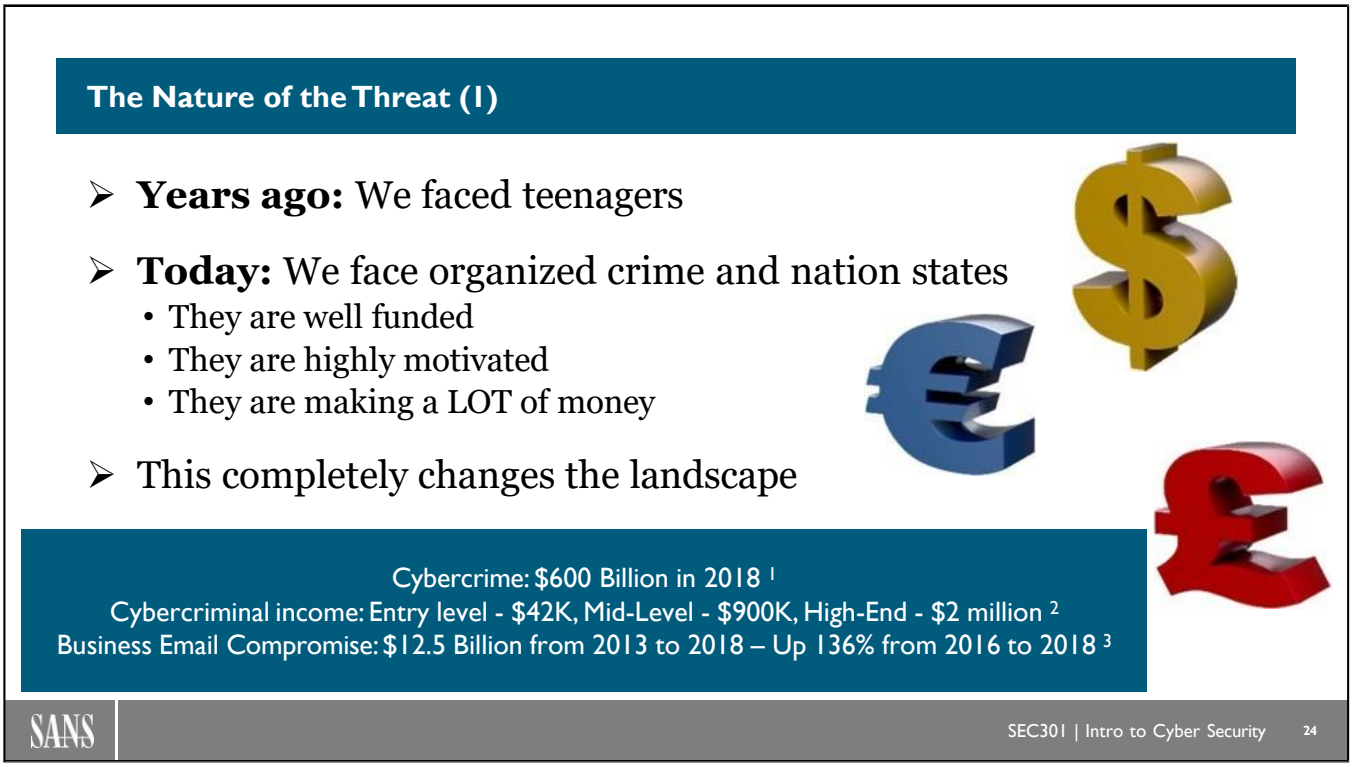
SANS SEC301 | Intro to Cyber Security 23

Roles and Responsibilities (2)

The next role we need to look at is the *data owner* (sometimes simply referred to as *the owner*). This is the person with primary responsibility for a particular piece of data. For example, the head of payroll would typically be the data owner of the payroll database. It is the owner of the data who makes decisions about proper classification of the data and any protective measures that are needed.

The *data custodian* (or simply *the custodian*) is the person or group who actually protects the data. They make the protection decisions of the owner become reality. To return to the example of the payroll database, if the owner decides that group A should have read-only access, but group B needs read-write, then the custodian (a system administrator or database administrator) would put those permission settings in place. Note that custodians will often need to act as advisors to owners. The data owner may not know what security measures are possible.

Finally, we have the user. It is clear that this is the role of the person who actually uses the data. What is less obvious, but important, is that a user is always automatically a data custodian. While you are using data, you have a responsibility to protect that data; therefore, you are simultaneously acting in the roles of user and custodian.



The Nature of the Threat (1)

Thirty years ago, the primary concern in security was teenagers saving their lunch money for a year, so they could buy a 400-baud modem and dial in to hack something. Teenagers are certainly still out there, though today they have a high-speed internet connection. However, it is not teenagers we have to be most concerned with now.

The #1 and #2 threats against our systems today are organized crime syndicates and nation states. The Hiscox Cyber Readiness Report states that cybercrime cost over $450 billion globally in 2017.

This is no longer the teenager and their lunch money. This is now an adversary who has a bigger budget for this year than most of us will have in our careers.

With the advent and explosion of ransomware (total cost exceeded $5 billion in 2017, up over 350%), money has become the number one motivating factor. Of course, that is not the only possible motivation. For example, the NotPetya ransomware, while it infected organizations worldwide, was clearly targeted at Ukraine.[4] The attack took out critical infrastructure services there such as the power grid and was clearly geopolitically motivated.

[1] https://www.hiscox.com/sites/default/files/content/documents/2021-Hiscox-Cyber-Readiness-Report.pdf

[2] https://www.infosecurity-magazine.com/news/cybercriminals-earn-millions/

[3] https://www.ic3.gov/media/2018/180712.aspx

[4]https://qz.com/1015755/ukraine-cyber-attack-the-petyapetrwrap-ransomware-with-similarities-to-wannacry-is-now-going-global/

See also:
https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

The Nature of the Threat (2)

- **Disgruntled Insider:**
  - Difficult to counter
  - Tends to be subtle
  - Often damaging or even devastating

- **Accidental Insider:**
  - Common – User clicks a link
  - No intent to cause harm
  - In aggregate, more damaging than disgruntled
- **External Insider:**
  - Outside threat source
  - Accidental inside threat actor:
    - End result of the accidental insider
    - The most-common attack vector

The Nature of Threat (2)

The fact that we face an insider threat has not changed over the years. The nature of the insider threat certainly has. As a general rule, the disgruntled employee has a much higher degree of technical skill than we faced in the past. Even if their skill level is not that high, information on how to cause damage is readily available through an internet search engine. And you cannot allow yourself to forget that a sledgehammer or a chainsaw can be very damaging to computer equipment and require extremely low skill levels to operate.

Part of the problem with the disgruntled insider threat is that they are insiders and they are disgruntled (we know, this sounds repetitive). In other words, someone in the company that we have already granted some level of access to has become unhappy with us. They know exactly how to hurt us badly, and because they are unhappy, they are motivated to hurt us badly. That is a dangerous combination. In fact, there are numerous cases of disgruntled employees bankrupting companies.

More recently, the discussion of insider threat expanded to include two new categories. First, the accidental insider: a user on our network that has no intention of causing damage, but does so by accident. Two of the most common ways they create that damage is by opening email attachments or clicking links in email messages. Visiting dangerous websites would come in a close third. In any case, they cause the damage when malware enters the network because of their accidental actions.

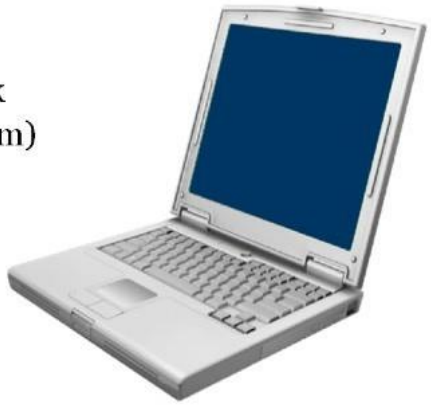
Very often, the malware infestation caused by the accidental insider grants remote control to an outside entity (an individual hacker, a cybercriminal, a nation-state actor, etc.). This leads

to the last category of insider threat: The external insider—the individual or group that has gained remote control access to at least one computer inside your network. So, they are physically located external to your network, but their access is identical to that of an internal user. Hence the name *external insider*.

Lab Time

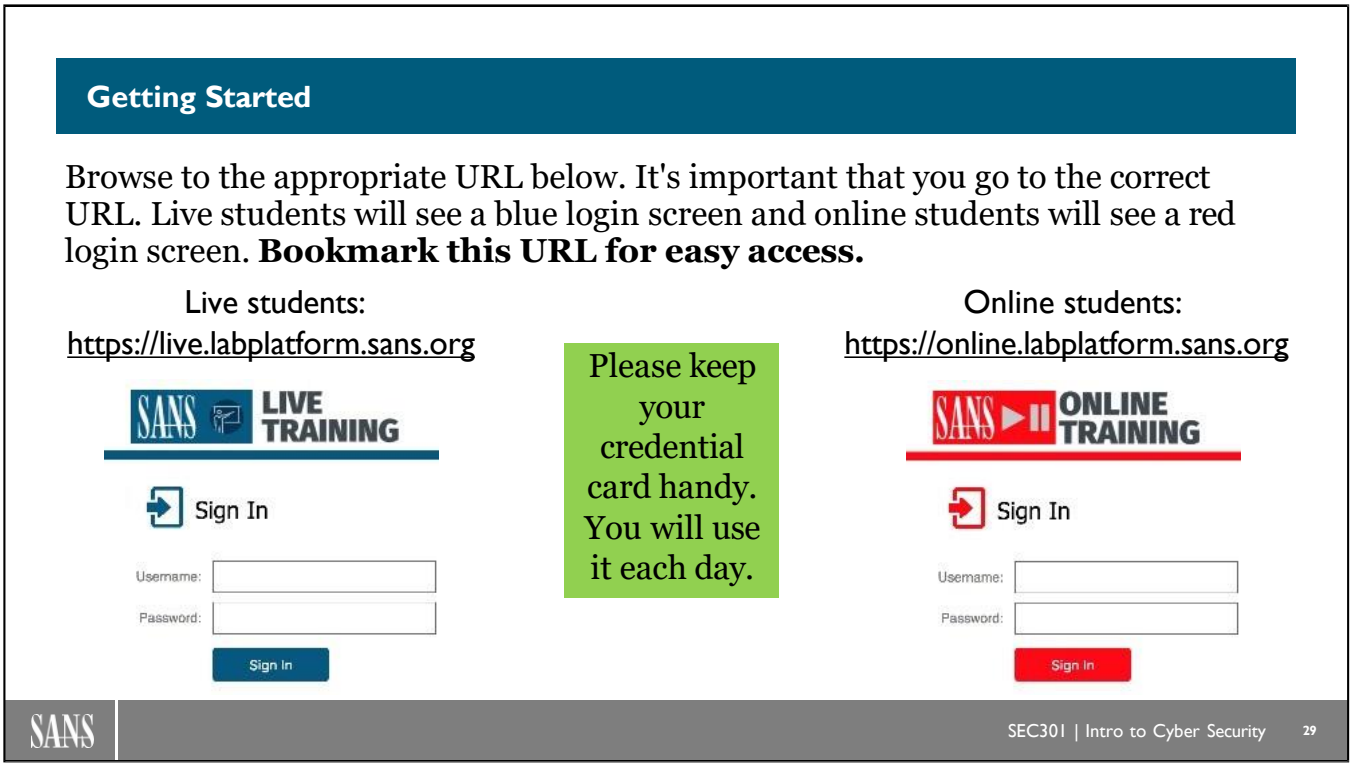
- LAB 1.1: Introduction to LODS and Quizzes

- Objectives:
  - Ensure connection to the classroom net work
  - Introduce the LODS (Lab On Demand S ystem)
  - Introduce the Module Quizzes



- Estimated completion time: 20 minutes

Lab Time:
LAB 1.1: Introduction to LODS and Quizzes



Getting Started

In the beginning of class, your instructor will hand out login credentials with your username and password information needed to access the lab server. Please keep this information handy, as you'll use it each day for labs.

Simply browse to the URL on this page. When prompted, enter your username and password information, then click Sign In.

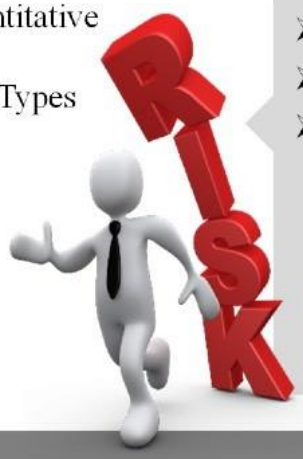
If you are completing the course as a SANS Online student, SANS will send you an email with your account access credentials.

For both online and classroom students: You can access additional materials that are not used in the classroom by going to the website below and entering the login information provided.
http://www.sec301.com
Username: student
Password: asimplepassword

This website will change over time with the quizzes and videos being updated, and possibly other material being added. The sec301.com website is not officially part of the SEC301 course. The site provides supplementary information to help students.

Module 2: Risk Management

- Risk Management Introduction
- Qualitative / Quantitative
- Risk Calculations
- Control Area and Types
- Risk Strategies



COURSE ROADMAP

- Module 1: Core Principles
  - Lab 1.1: Introduction to LODS and Quizzes
- **Module 2: Risk Management**
- Module 3: Security Policy
- Module 4: Authentication, Authorization, and Accountability (AAA)
  - Lab 1.2: Building Better Passwords: The Haystack

Module 2: Risk Management

If you think about it, security is an exercise in Risk Management. The security program is about mitigating risk as much as possible while still allowing the organization to accomplish its mission.

So, we begin our discussions with the Risk Management program. The remainder of the course deals with methods of mitigating risk.

In this module, we cover:

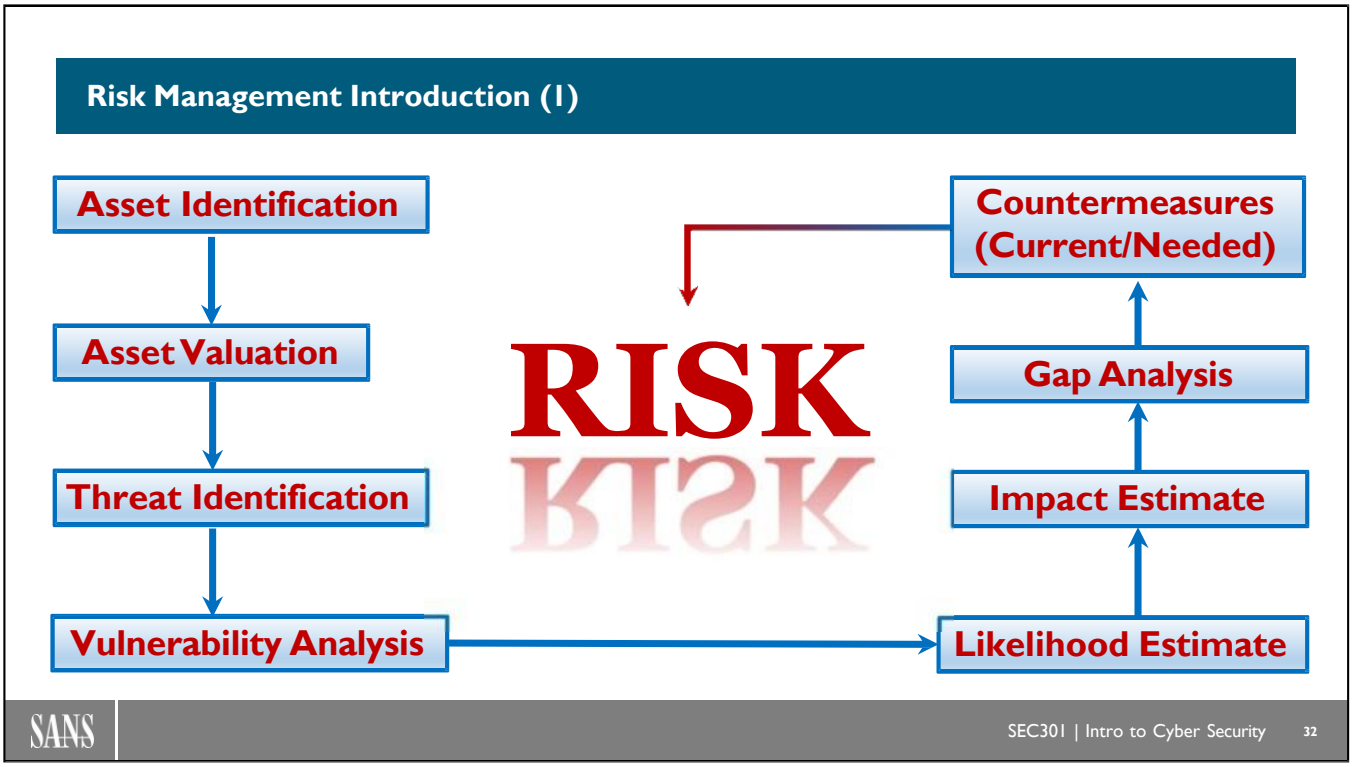
- Risk Management Introduction
- Risk Calculations
- Qualitative / Quantitative
- Control Types
- Risk Strategies

Risk Management Terminology

- **Threat:** Anything that can do anything bad to our stuff
- **Vulnerability:** Anything that allows the threat to happen
- **Likelihood and impact:** How likely is it to happen and how bad will it be?
- **Countermeasure/safeguard:** Anything to lessen or mitigate a vulnerability
- **Gap Analysis:** Here is our risk; here are our countermeasures. What is the gap between?
  - And how can we close the gap both effectively and cost-effectively?

Risk Management Terminology

To begin, we need to have some basic terminology. The terms on this slide are used throughout the discussion of Risk Management and indeed throughout the course.



Risk Management Introduction (1)
The term Risk Management is an umbrella term that encompasses all of the following:

- **Asset identification:** What are you trying to protect? Remember that you must identify both tangible assets (equipment, etc.) and intangible assets (data, reputation, etc.).
- **Asset valuation:** How important is the asset? An accurate estimate is difficult, but we will discuss some reports that can now be used to make more accurate estimates.
- **Threat analysis:** What threats or dangers concern us?
- **Vulnerability analysis:** Which of those threats can cause problems?
- **Likelihood:** How likely are those threats to happen? The likelihood is a moving target that changes over time.
- **Impact:** If/when they do happen, how bad will they be?
- **Gap analysis:** Is there a gap between the problem and our protections? If so, how do we close that gap in the most efficient and most cost-effective ways possible?
- **Countermeasure identification:** How can we most effectively close the gap?

When we take all these factors together, we can determine our level of risk. We must then ask, "Is the level of risk too high?" Has the organization met the minimum Standard of Due Care?

Risk Management Introduction (2)

- Risk management is performed in large part due to the legal obligations of the company—the Senior Manager in particular
- **Prudent Person Rule**:
  - Did the organization act as a prudent person would act in protecting assets?
- **Due Diligence**:
  - The industry best practices considered prudent
- **Due Care**:
  - A legal standard
  - Actions that a reasonable person would exercise to protect assets

Can the Senior Manager convince a judge that they followed the Prudent Person Rule in implementing Due Diligence to meet the Standard of Due Care?

And will the judge agree?

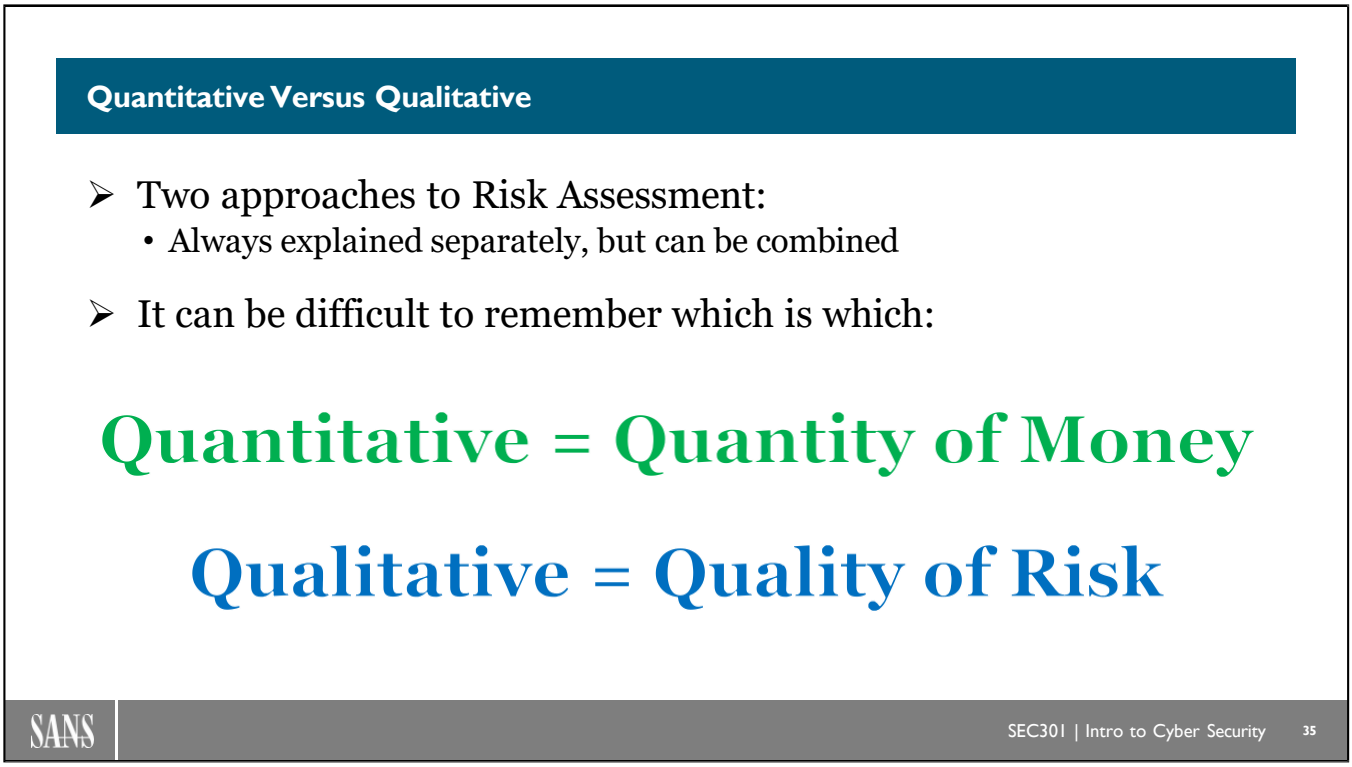
Security Manager only advises!

Risk Management Introduction (2)

There are legal requirements for an organization (the Senior Manager in particular) to protect the assets of the organization and to maintain the organization as a viable entity. This is true of every company regardless of size, but the requirements and penalties increase for larger companies. They become especially important for any publicly traded company.

- In court, the judge will look at the Prudent Person Rule to determine if the organization "acted as a prudent person would act" in protecting the assets of the organization.
- In meeting the prudent person rule, the organization practices Due Diligence. This means that the organization is following appropriate best practices in meeting Due Care. To say it another way, this includes all the things you do when you are trying to do the right thing.
- If the organization implements due diligence in meeting the Prudent Person Rule extremely well, they may be seen as meeting the legal Standard of Due Care.

Can the Senior Manager convince a judge that they followed the Prudent Person Rule in implementing Due Diligence to meet the Standard of Due Care? And will the judge agree?



Quantitative Versus Qualitative

There are two approaches to conducting a Risk Assessment: Quantitative and qualitative. We will discuss each of them in turn.

Because the names are so similar, some people have difficulty remembering which is which. Perhaps it will help to remember it this way:

- Quantitative Risk Assessment deals with the Quantity of Dollars.
- Qualitative Risk Assessment deals with the Quality of the Risk.

Why those statements are true will become apparent as we explain the details of each. We will begin on the following page with Quantitative.

Risk Calculation Terms

Quantitative = Quantity of $$$

* Means multiply

- Asset Value (AV) ➔ self-explanatory
- Exposure Factor (EF) ➔ 0% to 100% loss to AV
- Single Loss Expectancy (SLE) ➔ AV * EF%
- Annual Rate of Occurrence (ARO) ➔ Based on research
  - How often will a threat occur on an annual basis?
  - ARO examples: 0.0 (never), 0.04 (every 25 years), 0.5 (every other year), 1.0 (once a year), 2.0 (twice a year), 2.5 (two-and-a-half times a year), and so on
- Annual Loss Expectancy (ALE) ➔ SLE * ARO
  - SLE annualized

http://www.riskythinking.com/glossary/

SANS | SEC301 | Intro to Cyber Security 36

Risk Calculation Terms

In conducting the Risk Assessment, a number of calculations are necessary. We use these to determine the appropriate expenditures for countermeasures. You need to understand several terms to perform the calculations:

Asset Value (AV): The term is self-explanatory. However, determining asset value is not nearly so simple. Some things are tangible and easy enough to value, such as computers, software, and equipment. You have a receipt for all of that. Less easy to value are the intangibles, such as your data. What is actually the value of that database?

This is incredibly difficult to do well but also vitally important to get right. Clearly, you would not spend a million dollars to protect a $10 asset. But you also do not spend a million dollars to protect a million-dollar asset. Every dollar you spend on protection devalues the asset by that amount. So, if you have a million-dollar asset and spend a million to protect it, the end result is a zero-dollar asset.

Exposure Factor (EF): The percentage of the asset value lost if a particular risk is realized. In other words, how much of the asset would you lose if the "bad thing" happened? Note this is expressed as a percentage between 0% and 100%. So, if you have a $500,000 building and a fire damages 10%, you have a 10% EF, which is $50,000. (As you will soon see, that is a simplification, but that is the concept.)

Single Loss Expectancy (SLE): How much will it cost each time the threat happens? If you take the Asset Value (AV) times the Exposure Factor (EF), you have the Single Loss Expectancy. In the previous example of the fire in the building, we took the AV of $500,000 times the EF of 10% to arrive at the $50,000 SLE.

Annual Rate of Occurrence (ARO): How many times a year do you expect a particular threat to occur? That number is the ARO. Note that ARO is often greater than 1 (once a year) but can also be less than 1 (every 10 years, for example). When expressing ARO, you do so by a number:

- 2.0 = Twice per year
- 1.0 = Once per year
- 0.5 = Every other year
- 0.2 = Every 5 years
- 0.1 = Every 10 years
- 0.05 = Every 20 years
- 0.04 = Every 25 years

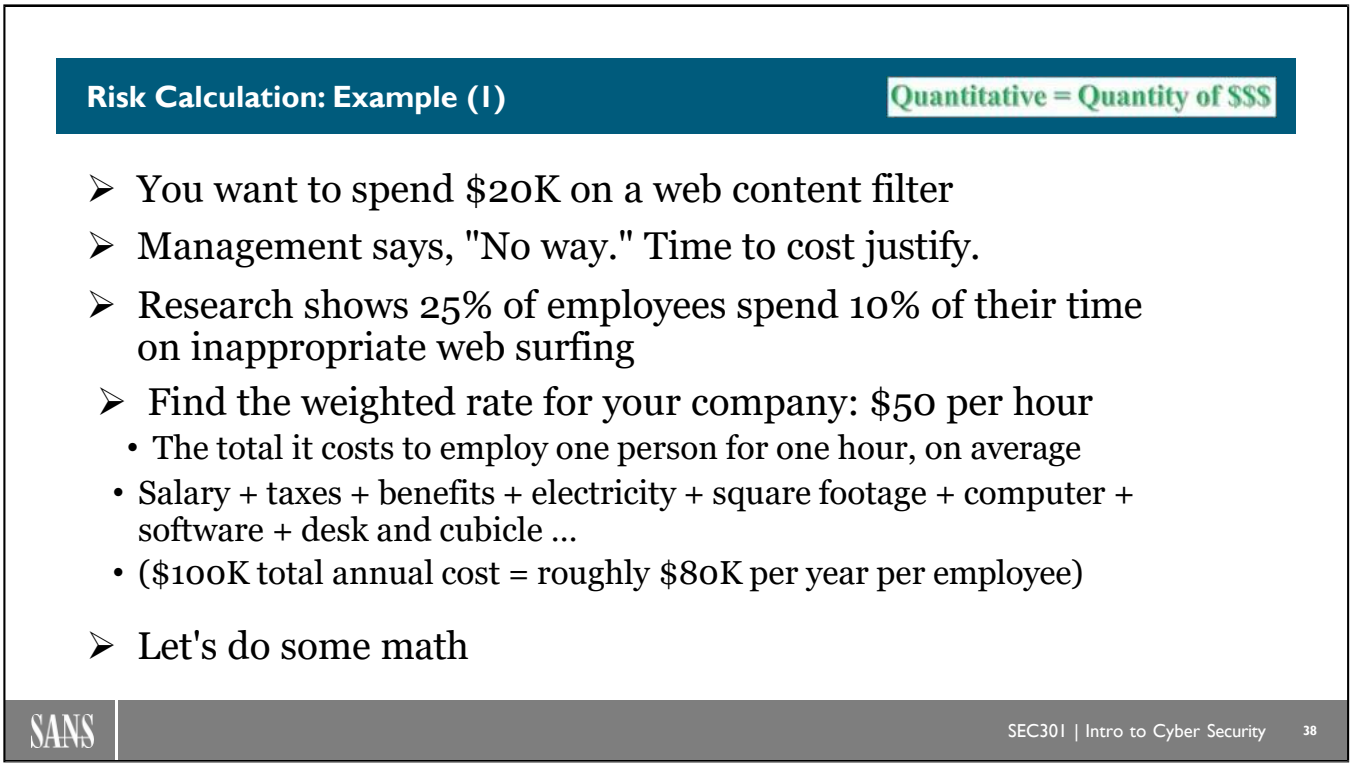
The problem with ARO is that you have to predict the future to get it right. Of course, you can't accurately predict the future. How many attacks will your organization face next year? How often will you have a fire in your data center? The best you can do is conduct research and make the most educated guess possible.

Annual Loss Expectancy (ALE): This is the number we have been working toward: What everything else feeds into. It is effectively the Single Loss Expectancy annualized. You calculate it by taking the SLE times the ARO. This gives you the Annual Loss Expectancy (ALE). This also gives the best indicator of how much you can justify spending to mitigate a particular problem. If your research and calculations show that a particular vulnerability is going to cost you $10,000 per year, you can justify spending up to that amount to prevent the loss.

Using some simple numbers, let's assume we have a $5,000 asset and an Exposure Factor (EF) of 20%. That gives us an SLE of $1,000 ($5k * 20%). So, if we take that with different AROs, we arrive at the Annual Loss Expectancy (ALE):

- 2.0 = twice per year — $1,000 x 2 = $2,000 ALE
- 1.0 = once per year — $1,000 x 1 = $1,000 ALE
- 0.5 = every other year — $1,000 x 0.5 = $500 ALE
- 0.2 = every 5 years — $1,000 x 0.2 = $200 ALE
- 0.1 = every 10 years — $1,000 x 0.1 = $100 ALE
- 0.05 = every 20 years — $1,000 x 0.05 = $50 ALE
- 0.04 = every 25 years — $1,000 x 0.04 = $40 ALE

You can find these terms (and more) with their definitions at http://www.riskythinking.com/glossary/



Risk Calculations (3)

Now take a look at an example of how to apply these calculations.

You have a concern that some employees spend too much time on inappropriate web surfing. You approach management and ask for funding to implement a web content filter. The cost would be $20,000. Management does not feel there is enough justification. (Some people are just going to some websites after all.) It is time to cost justify.

If you actually conduct research on this issue, it is estimated that approximately 25% of employees spend approximately 10% of their time on inappropriate web surfing. We will use these numbers for our example.

You meet with the head of accounting to find out the weighted rate for your company. This number is what it costs (in total) per hour for the company to employ one average person. The weighted rate includes salary, taxes, benefits, the employee's electricity use, the cost of their desk/cubicle, and the square footage it takes up, the cost of their computer and software and such ... literally everything it costs to employ one person for 1 hour.

The head of accounting gives you the figure of $50 per hour weighted rate. That number sounds high, but it really isn't. If you take 40 hours per week times 52 weeks, that equals 2,080 hours in a work year. Fifty dollars per hour times 2,080 hours equals $104,000.

Depending on the area of the country, benefits, and several other factors, that equates to an $80,000 per year employee. (Take your annual salary and add 25%. You are not too far off the mark from your weighted rate for your organization to employ you.)

You now have the raw numbers you need for the calculations, which we will perform on the next slide.

Risk Calculation: Example (2)

Quantitative = Quantity of $$$

- 25% spend 10% of their time:
  - Company has 1,000 employees
  - Company has a $50 weighted rate
- 1,000 employees x 25% = 250 people
- 40-hour week x 10% = 4 hours a week each
- 4 hours x 250 people = 1,000 hours a week total
- 1,000 hours x $50 per hour = $50,000 weekly SLE
- $50,000 per week x 50-week work year = **$2,500,000 ALE**

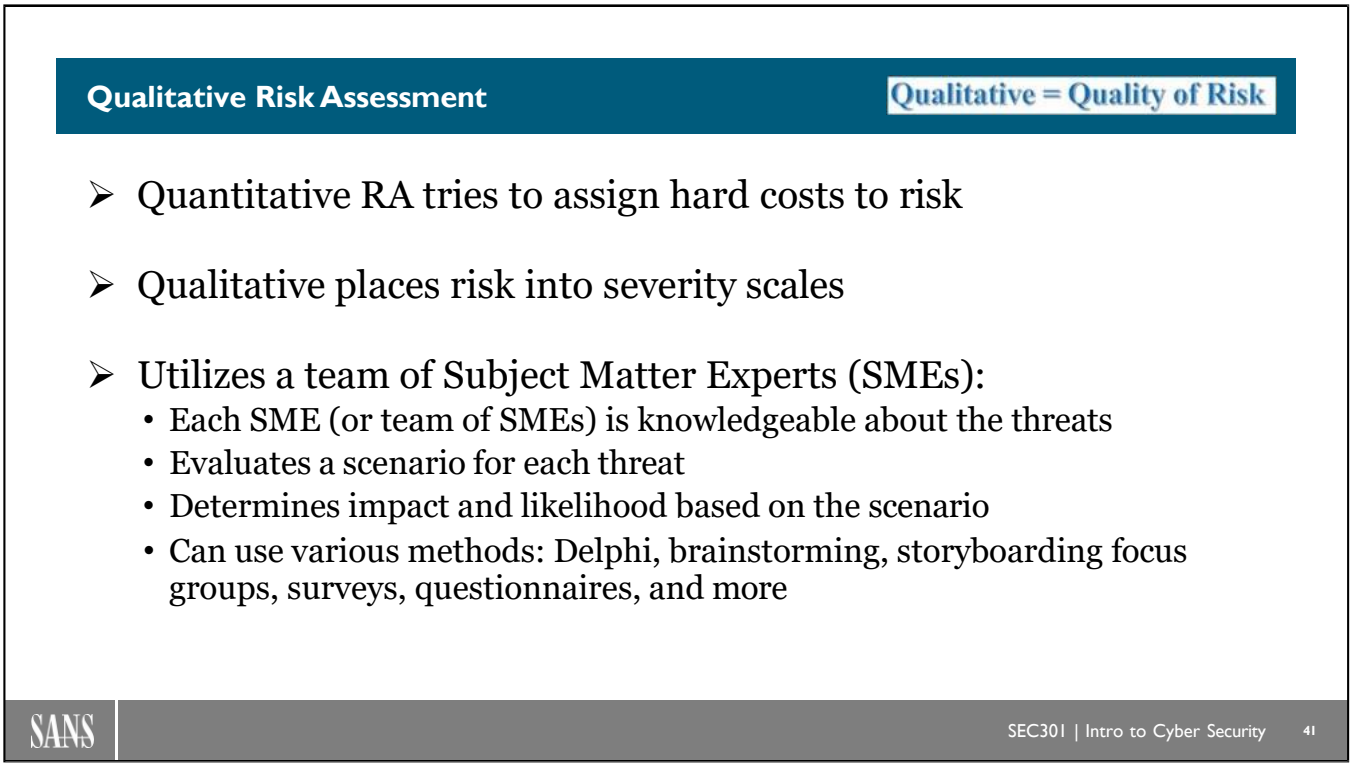
Cost Justification!

Risk Calculation: Example (2)

If 25% of 1,000 employees spend 10% of a 40-hour week surfing to bad places, that is a total of 1,000 hours per week across the company. Take that 1,000 times the weighted rate of $50 per hour and you have a weekly SLE of $50,000. (SLE is not always weekly, but it is the easiest way to figure it in this example.)

Figure a 50-week work year (2 weeks are for vacation): 50 times $50k = $2,500,000 Annual Loss Expectancy because some folks decided to "just spend a few minutes" going to non-business websites.

When you return to management and show them these numbers and then ask for $20,000 to prevent a $2.5 million loss, you are much more likely to get the budget. That is how you perform cost justification.



Qualitative Risk Assessment

Although the Quantitative approach tries to assign hard costs to risk, the Qualitative approach places risk into severity scales. Instead of a million-dollar threat, you have a level 10 threat.

To accomplish this, utilize a team of Subject Matter Experts (SMEs). Each SME or group of SMEs is hopefully knowledgeable about the threats your organization faces. If they are not, then the term *SME* does not apply to them. In this case, you may have to create SMEs through education.

You would typically create a questionnaire for each threat/vulnerability and have the SMEs answer the questionnaire. You collect the questionnaires and see if you have something approaching consensus.

The questionnaire asks each SME to rate the likelihood and severity of each threat on a numbered scale. The process looks something like the following.

The Delphi method is a systematic, interactive forecasting method that relies on a panel of experts who answer questionnaires in two or more rounds. After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round, as well as the reasons they provided for their judgments. It is believed that during this process the range of the answers will decrease, and the group will converge toward the "correct" answer. Finally, the process is stopped after a predefined set of rounds, and the mean or median scores of the final rounds determine the results.

Qualitative Risk Ranking

Qualitative = Quality of Risk

Scale 1-5		
Threat: Virus		
	Likelihood	Severity
SME #1	5	5
SME #2	4	2
SME #3	1	4
SME #4	5	5
Average:	**3.75**	**4**

Note: SME #3 may not understand virus likelihood and #2 may not appreciate the severity. If you have several SMEs, it is sometimes best to throw out the high and low scores and then calculate the average. Here, that would give 4.5 likelihood and 4.5 severity—both round to 5—so 25 on the scale.

SANS SEC301 | Intro to Cyber Security 42

Qualitative Risk Ranking

When conducting Qualitative Risk Analysis, you work with a team of Subject Matter Experts or SMEs. You and the SMEs first determine each specific vulnerability you are concerned about. You then prepare a questionnaire for each concern and have your SMEs rate the Likelihood and Severity. You collect the questionnaires and average the responses. Round the averages, and place them into the scale on the right in the appropriate spot.

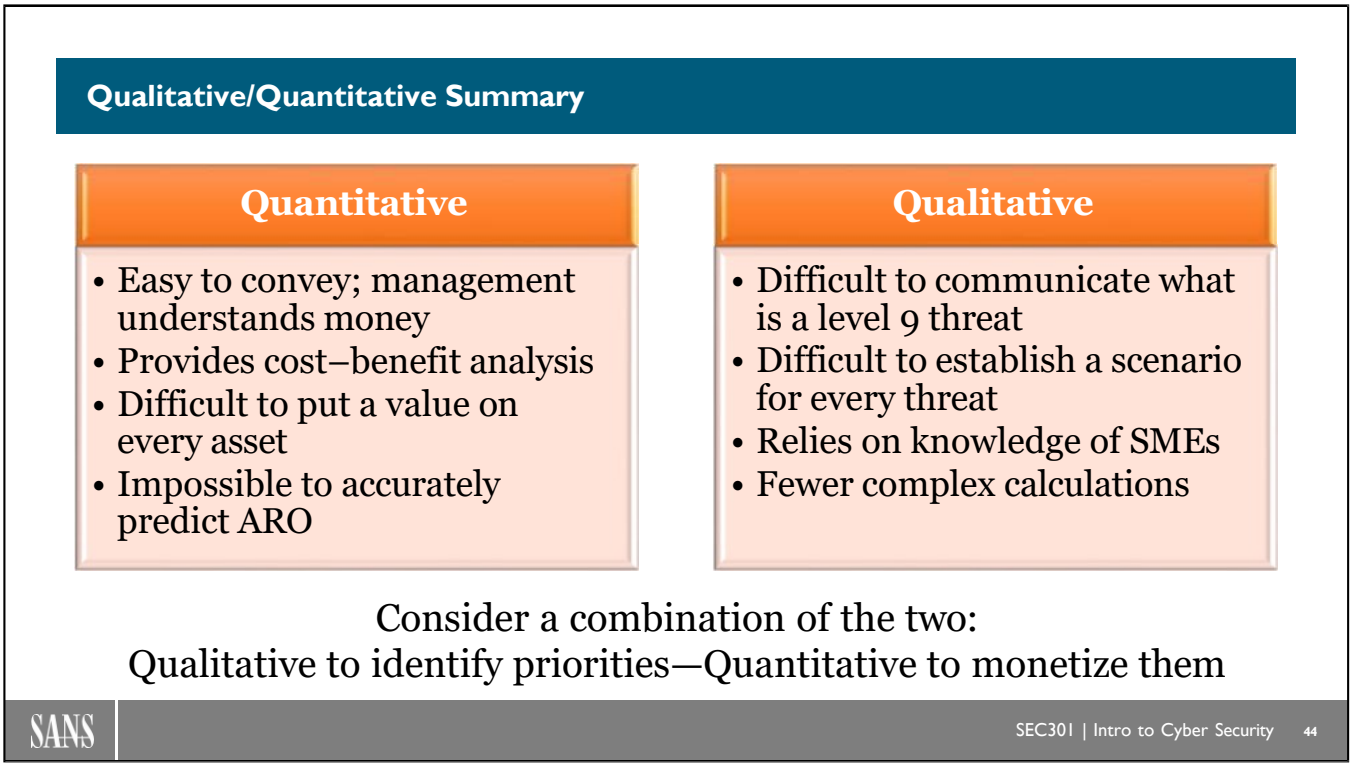
Unfortunately, not all SMEs will have equal knowledge. They may over or underestimate the Likelihood or Severity. Provided you have enough SMEs in the group, you can throw out the high and low in each category and then average the results again. This will often get you a more realistic answer. Note that five SMEs is the absolute minimum number for this to work, and you need at least six before it is effective.

On the Risk Assessment Scale from top to bottom, you have Likelihood on a numbered scale. Across the bottom, you have Severity on a numbered scale. In this case, we are using a 5 by 5 scale. Meaning that for Likelihood, we have a scale of 1 through 5. The Severity scale is also 1 through 5. You could think of these numbers as critical, high, medium, low, informational (from 5 down to 1 obviously).

Risk = Likelihood X Impact (Risk equals Likelihood Times Impact)

The above formula demonstrates that Risk is calculated by multiplying the likelihood of a threat by its impact on security. To determine a risk score, you simply multiply the likelihood

value by the impact value. The higher the risk value, the more significant the risk. Applying this formula to different potential threats gives you a prioritization of each risk. You would want to address the highest numbered risks before worrying about the lower risks.



Qualitative/Quantitative Summary

Both Qualitative and Quantitative approaches have their good points and their bad points. You need to understand them both.

Quantitative lends itself to easier communication with management. "Boss, we have a million-dollar risk" is much easier to understand than "Boss, we have a level 9 risk." The Quantitative method also lends itself to cost justification, as shown earlier.

However, we also explained how difficult it can be to identify all the assets and put correct values on them. Then there is the problem of accurately predicting the ARO.

Qualitative also has a precognition (predicting the future) element when you try to estimate the likelihood, rate of occurrence, and impact. With a team of SMEs, we hope that these estimates are closer to reality. There are fewer complex calculations with Qualitative. Some believe the more straightforward calculations make Qualitative easier as well.

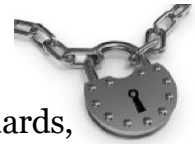
One point on Qualitative Risk Assessment: It relies on the quality of the SMEs involved. Not all Subject Matter Experts deserve the E in that title. Honest assessment of the level of knowledge of the SMEs is a critical part of that process.

Some organizations choose to conduct a combination of these strategies. For example, you might use Qualitative to identify the top 20 concerns and then apply Quantitative to monetize those concerns. This combined risk assessment process is very common in the security industry.

Control / Countermeasure / Safeguard: Areas & Types

Control Areas

- Administrative
  - Policy, Procedure, Awareness
- Technical
  - Firewall, Crypto, Permissions
- Physical
  - Guns, Gates, Guards, Locks, Lighting, Cameras



Control Types

- Prevent
  - Authentication, Firewalls
- Detect
  - Logs, audits, Intrusion Detection
- Respond
  - Incident response

Prevention is ideal
Detection is a must
Detection without response is useless

SANS | SEC301 | Intro to Cyber Security 45

Control / Countermeasure / Safeguard: Areas & Types

Part of the Risk Management process is determining ways of lowering the risk to the organization. There are three terms you will hear for this; they are interchangeable:

- Control / Countermeasure / Safeguard

There are Control Areas and Control Types. They are similar, but different.

Controls Areas are:

- Administrative controls
  - Think paper
  - Policy, procedure, standards, guidelines, and compliance
  - Awareness training is not totally paper-based but also falls in this area
- Technical controls
  - Firewalls, antivirus, encryption, and such. Things that are technical or technology
- Physical controls
  - Guards, guns, gates, locks, fences, lighting, fire suppression, Closed Circuit TV (CCTV),
  - Heating Ventilation and Air Conditioning (HVAC) and humidity controls

The key is to choose a combination of these control areas that will most effectively close the gap between the current level of protection and the level of risk. Note that control areas rarely, if ever, stand alone. Take, for example, backups: We have an Administrative control of policy that says we will do backups. We have a Technical control that is the backup software. We have a Physical control of the safe were we store the backups securely. You will almost always hit on at least the first two.

We have already discussed the three **Control Types**; we just didn't use that term when we did.

- Preventive
  - Authentication, firewalls
- Detective
  - Logging/auditing, Intrusion Detection Systems
- Corrective
  - Incident response plans, backup/recovery capability

These three control (or countermeasure, or safeguard) types highlight one of the most important points of this entire course.

Prevention is ideal
Detection is a must
Detection without response is useless

Risk Strategies (1)

- Risk Mitigation:
  - Just what it sounds like: Determine and implement countermeasures
  - You should always do this as long as it makes good business sense
- Risk Avoidance:
  - Stop the activity that causes the risk:
    - Since there are more viruses for Windows, switch to Mac or Lin ux
    - Put the data center on a hill instead of in a flood plain
- Risk Deterrence:
  - Implement detection and reaction capabilities:
    - Camera surveillance and prosecution of trespassers
    - IDS and terminate employees for unauthorized network scans

Risk Strategies (1)

We have looked a lot at how to identify our level of risk. Now let's look at the possible management decisions regarding that risk. The Senior Manager of the organization may decide to do any of the following:

- Risk Mitigation:
  - You need to implement more countermeasures to further mitigate (or lower) the level of risk
  - Meaning that management needs to give you more budget and manpower
- Risk Avoidance:
  - Stop the activity that causes the risk:
    - Windows has viruses, so let's use Mac (which has fewer)
    - A hurricane can't take out the data center if we put it in Denver
    - Let's not put our data in the cloud
- Risk Deterrence:
  - We will detect wrongdoing and take swift, decisive, and harsh action:
    - Prosecuting trespassers and/or hackers
    - Firing employees for inappropriate use of systems/resources

(This list continues on the next slide.)

Risk Strategies (2)

- Risk Acceptance:
  - You mitigate, avoid, and deter as much as you can
  - What you can't do the above for is *residual risk*
  - There will always be some of this—and you accept that risk
- Risk Transference or Risk Sharing:
  - Take the residual risk and transfer it to an insurance company
  - Expensive proposition; check the fine print carefully
- Risk Ignore-ance:
  - Sorry, this one is not allowed, even if management would prefer to do so
    - This is currently a huge problem in smaller companies–but 47% of attacks target small companies

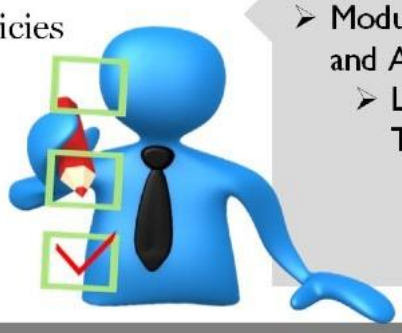
Risk Strategies (2)

- Risk Acceptance:
  - We have mitigated all we can afford to mitigate
  - We will accept the residual risk
  - Some level of this will always be necessary:
    - Some risks cannot be mitigated at any cost
    - Some risks can be mitigated, but not at a reasonable cost
- Risk Transference or Risk Sharing:
  - We perform all the mitigation we can
  - We accept the residual risk
  - We buy insurance to transfer the risk to someone else – or share the risk with someone else:
    - Most common today in the financial sector

Notice there is one here that is *not* allowed. Risk Ignore-ance (or ignoring risk). You cannot do that one, *AND* you cannot let your management do it either. The approach of "Risk? What risk? I don't see any Risk!" was common years ago but not effective. The world today will simply not allow for it.

Module 3: Security Policy

- Security Policy Introduction
- Privacy Policies
- Acceptable Use
- Personnel Policies
- Data Specific Policies



COURSE ROADMAP

- Module 1: Core Principles
  - Lab 1.1: Introduction to LODS and Quizzes
- Module 2: Risk Management
- **Module 3: Security Policy**
- Module 4: Authentication, Authorization, and Accountability (AAA)
  - Lab 1.2: Building Better Passwords: The Haystack

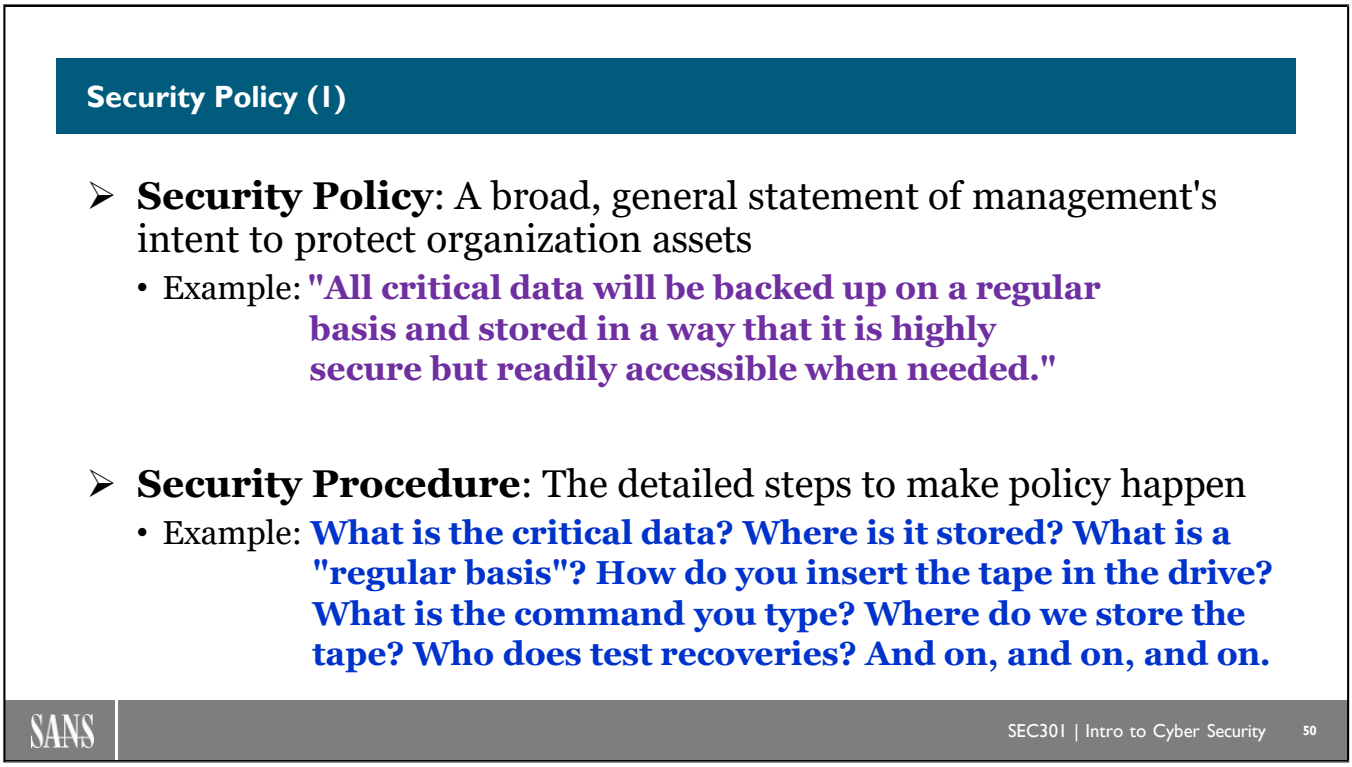
SANS SEC301 | Intro to Cyber Security 49

Module 3: Security Policy

One of the most important parts of any security program is the security policy. It is the foundation of the entire rest of the program.

In this module, we discuss:

- Security Policy Introduction
- Privacy Policies
- Acceptable Use
- Personnel Policies
- Data Specific Policies



Security Policy (1)

At the most fundamental level, a security policy is a broad, general statement of management intent. You do not want a security policy to be highly detailed because that would require frequent changes and updating.

An example of a good backup policy for a typical organization might read: "All critical data will be backed up on a regular basis and stored in a way that it is highly secure but readily accessible when needed."

You may be saying, "Gosh, I have a backup policy at work that weighs 72 pounds." That is not your backup policy; those are your backup procedures. The procedure documents spell out, in this example, what the critical data is and where it is stored, what is a "regular basis," how to insert the tape in the drive, what is the command you type, and so on.

In other words, the policy is the broad, general statement of intent. Procedures are the detailed steps necessary to make that intent a reality.

Security Policy (2)

- Good policy: 20 to 50 pages
  - Or better yet, 20 to 50 one-page policies:
    - Each is specific to one issue
    - Simplifies managing signature process—no small issue!
- *Clear*, *concise* writing:
  - No **technical jargon**. No **sesquipedalian writing**.
- Wording must be *directive* in nature:
  - ***Must***, ***shall***, and ***will*** are requirements (and will be *audited* as such)
  - *Should, might,* and *can* are suggestions

Security Policy (2)
If you keep with the broad, general statement type of policy, a good security policy for most organizations would be 50 pages or less.

Better yet, 50 one-page documents. Doing each policy in a stand-alone document makes it a lot easier to maintain. Keep in mind that only the Senior Manager can sign policy documents. Getting that signature can be a major hurdle, especially in large organizations. The document must go through all levels of management before making it to the Senior Manager. Each level of management can request changes, which means you have to start the process over.

If one of those higher-level managers does not want your policy to make it to the Senior Manager (perhaps they don't like your strong password policy), they can block it forever. By having separate stand-alone documents, blocking you is more difficult. If you are asking only for approval of the backup policy, they cannot (as easily) require changes to the password policy, which is in a separate document.

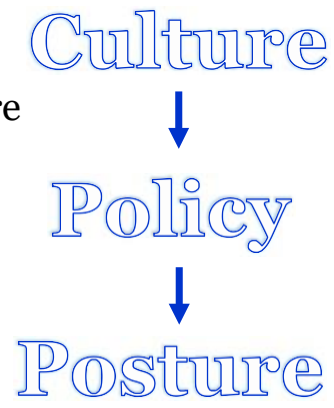
A security policy should be written in the clearest terms possible. This is not the time for sesquipedalian writing. (See below for definition.) You should also avoid technical jargon as much as possible.

Finally, it is important that you use directive language. A security policy is a legal document. In court, there is a huge difference between *must, shall,* and *will* (which create requirements) and *should, might,* or *can* (which make non-compulsory suggestions).

Note: Sesquipedalian (pronounced ses-kwə-pə-ˈdāl-yən) is defined by the Merriam-Webster dictionary as "given to or characterized by the use of long words." And we think that makes our point quite well. ☺

Security Policy: Culture vs. Posture

- Corporate Culture defines the security policy:
  - E.g., personal use of email, laptop, etc.
- If the culture is anti-security, change the culture
  - Policy is passive—it does not force change
  - You cannot change culture by writing policy!
  - Only when culture supports policy can policy be effective
- Culture driven Security Policy defines the Security Posture:
  - How secure is an organization
  - What is the risk tolerance

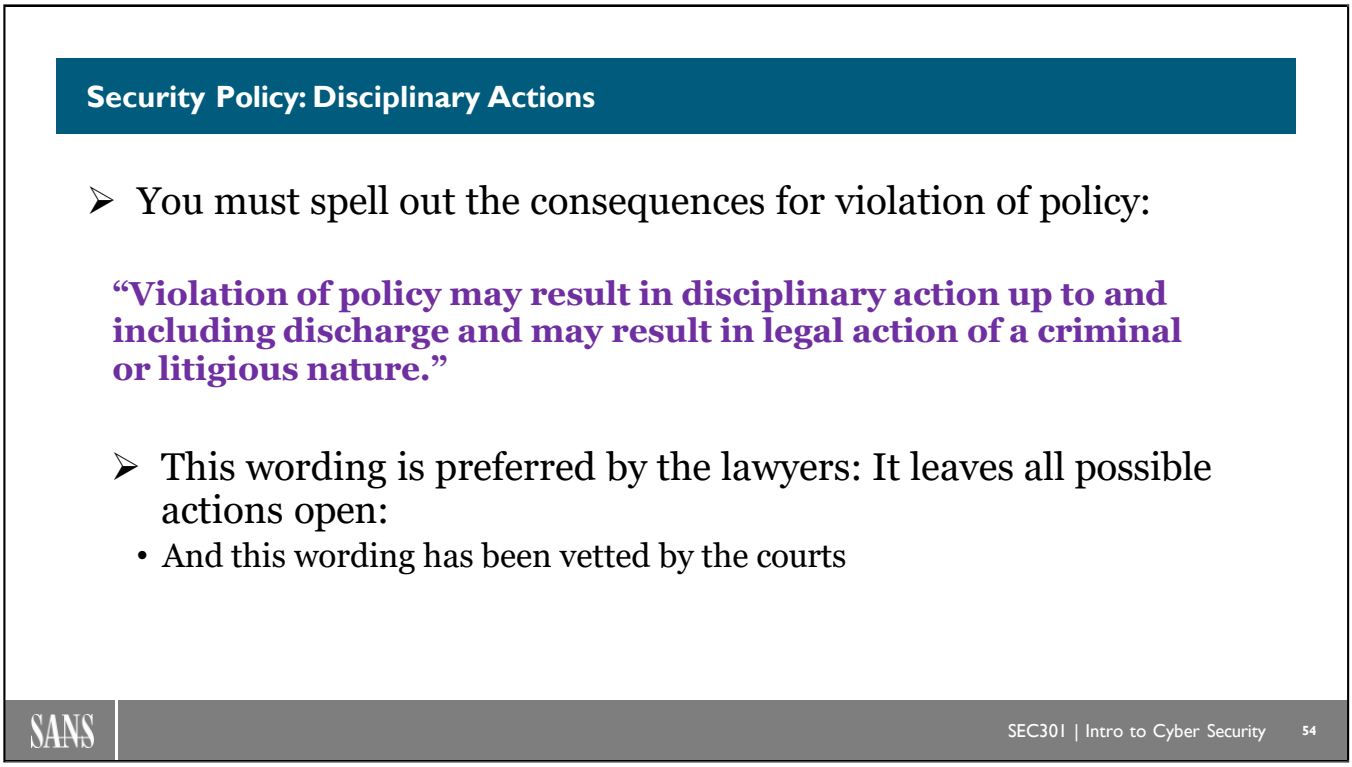


Security Policy: Culture vs. Posture

The corporate culture defines the security policy of an organization. For example, will you allow employees to make personal use of email or a laptop? In some corporate cultures, this is expected. In others, it is forbidden. Always remember that you can never change the corporate culture by writing policy. You have to change the culture, then write the policy to match that culture.

The security policy defines the security posture of the company. It is a completely passive form of security in that it does not actually enforce anything. But it does spell out what is supposed to be enforced.

The security policy applies to every individual with access to any portion of your network through any means. Portions of your security policy such as that dealing with physical security will also apply to non-computer users (maintenance staff, janitorial staff, and others).



Security Policy: Disciplinary Actions

As a legal document, your policy will undergo legal review. You can write the section on sanctions in any way you like. However, when you get it back from the legal department, this is what it will almost certainly say:

"Violation of corporate policy may result in disciplinary action up to and including discharge and may result in legal action of a litigious or criminal nature."

This wording leaves every possible avenue open to the organization: It may or may not punish you. It may or may not fire you. It may or may not sue you. It may or may not prosecute you. And it may or may not choose to do any combination of the above or it may choose to do none of the above.

Since this wording has been used in many courtrooms in several countries and judges are happy with the wording, lawyers prefer this wording. The wording has been "vetted by the courts".

Privacy Policies (1)

- Personally Identifiable Information (PII)
- Personnel records:
  - Payroll
  - Social Security Number (U.S.), National Insurance Number (U.K.)
- Customer information:
  - Addresses
  - Credit card data
  - Credit reports

- Legal requirement in many U.S. states
  - Also required by federal regulations: HIPAA, GLBA, Sarbanes-Oxley As well as by PCI-DSS
- Legal requirement in many countries around the world

Privacy Policies (1)

Most privacy laws and compliance regulations require that an organization have privacy policies in place. Exactly which types you need depends on the type of information stored by your company.

Personnel records containing payroll information and Social Security numbers require protection in any company.

If your company accepts credit cards from customers, then there is a clear need to protect that information. Likewise, if you grant credit to your customers and pull their credit reports, you need to protect those.

Having sound policies regarding the protection of this type of information is an obvious requirement. In fact, it is a legal requirement in many cases. For example, in the United States:

- Healthcare organizations must comply with the law known as HIPAA (Health Insurance Portability and Accountability Act)
- Financial institutions have to comply with the law GLBA (Gramm-Leach-Bliley Act)
- Any organization publicly traded on the stock market must comply with Sarbanes-Oxley (often referred to as SarBox, or simply SOX)

Any company that needs to accept credit card payments must comply with the Payment Card Industry Data Security Standard (PCI DSS). While PCI DSS is not a law, it is still effectively a requirement if accepting credit cards is a business necessity.

Privacy Policies (2)

- Is there any "expectation of privacy" on the company network?
  - The answer is "Yes" … unless policy clearly states "No"
  - The Electronic Communications Privacy Act of 1986 (ECPA) requires the following before monitoring employee activity:
    - Stating monitoring will be done
    - Who can do it and under what conditions
    - What will happen if something inappropriate is found
    - Documentation that all users are aware of the above
  - At that point, there is no expectation of privacy:
    - Employers can then monitor email, keystrokes, and more

U.S. Specific Info

Privacy Policies (2)

In the United States, your employees have an expectation of privacy regarding their activity on your network. This means that you cannot monitor their activity in any way.

That expectation of privacy continues until you (or more specifically the company) notify the employee in a formal and documented way that there is NO expectation of privacy. This notification is an important part of the awareness program.

The preceding information is from a U.S. federal law called the Electronic Communications Privacy Act (ECPA). Before the company can legally monitor employee activity, all the following must be in place in a written statement (part of policy):

- Stating monitoring will be done
- Who can do it and under what conditions
- What will happen if something inappropriate is found

In addition, there must be:

- Documentation that all users are aware of the above, which is one of the reasons awareness training requires documentation

British & EU Privacy Laws

- Britain and all EU countries:
- General Data Protection Regulation (GDPR)
  - Took effect May 25, 2018
  - Includes tougher guidelines on protecting privacy and reporting breaches
  - If your company provides goods and/or services or collects and stores information on anyone located in the EU, you must comply with GDPR
    - Even if you don't have offices in the EU!
  - Much higher penalties **(20 million Euros or 4% of global revenue, whichever is higher)**
    - E.g., the fine for Equifax would have exceeded $100 Million
- See http://www.eugdpr.org/ View all 99 articles of GDPR via the link in your notes

SANS SEC301 | Intro to Cyber Security 58

British & EU Privacy Laws

Until recently in the United Kingdom, privacy was covered under the Data Protection Act of 1998. We believe the British Government will enact a law very similar to the GDPR discussed below.

Britain and all EU countries are adopting the General Data Protection Regulation. It includes MUCH tougher guidelines for protecting privacy and reporting breaches.

- Every company (in any country) that provides goods or services to any European Union citizen must comply with the GDPR or face penalties.
- This law went into effect May 25, 2018. If you are not yet compliant, your company should prioritize this. The fines are huge!
- Penalties are 20 million Euros or 4% of global revenue, whichever is HIGHER.

Compliance with this regulation will require significant effort on the part of most organizations. The EU GDPR expands the definition of private information and lays out stringent requirements for its protection. Among other things, the EU GDPR requires reporting of breaches within 72 hours and allows for holding data processors directly liable.

Information on the EU GDPR is available at: http://www.eugdpr.org/
The full 99 articles are available at: https://gdpr-info.eu/

The author would like to thank Stephen Jones, SANS Director of U.K/Nordics (and an E.U. Lawyer) for providing information on British and E.U. legal issues.

Acceptable Use Policy (AUP)

- Dictates what is and is not proper use of company resources:
  - Formalizes corporate culture
  - Agrees with all other policies
- Must be part of awareness training:
  - Training must be documented
  - Failure to comply "may result in disciplinary action..." (earlier slide)
- The part of the security program most likely to cause grief for you:
  - A litigation minefield
  - No knee-jerk reactions can occur here

Acceptable Use Policy (AUP)

The Acceptable Use Policy must accomplish two things:

1. It formalizes corporate culture.
2. It must agree with all other policies.

Based on the corporate culture of some companies, non-work-related internet activities might be permissible. In other companies, that can be a fireable offense.

Like all policies, it is important that the dictates of an AUP be covered in awareness training. In some ways, this is one of the most important policy areas to cover thoroughly. And yes, it is important that employees know the possible penalties for noncompliance.

Keep in mind, one of the most common reasons for employee termination is violation of AUP. Before you can hold employees accountable, you have to tell them in clear terms what this policy requires.

Be careful with AUP enforcement. Make no knee-jerk reactions. Especially when there is a chance of terminating employment, you have to get this right. Not only because it is the right thing to do, but also because you can have personal liability. Wrongful discharge lawsuits are extremely common. If you make the decision that people are in violation of AUP and they are terminated, both you personally and the company can face legal liability.

Personnel Security: Introduction

- Security is, first and foremost, a people issue:
  - It is people who implement a huge part of the overall security posture
  - If you do not address personnel security, your program will not succeed

Personnel Security: Introduction

We must never allow ourselves to forget who actually implements a large part of our security posture … the users.

Every time users change their password, choose a good password over a bad one, lock their terminal before going to lunch, and a myriad of other things we ask them to do, they are implementing security posture.

If we want them to do that well, we have to train them—meaning this again ties to the awareness training discussion.

Understanding this is critical to the success of the security program.

Personnel Security Policies (1)

- The following policies/practices prevent nothing. However:
  - They do force collusion
  - Meaning two or more people must work together to perpetrate fraud
  - When you force collusion, fraud becomes less likely, not impossible
- **Separation of duties**:
  - No one person has control of critical processes from beginning to end
  - Example: The person who creates invoices does not pay invoices
- **Dual control**:
  - No one person can access information alone—it takes two people
  - Two locks on a door or safe, two passwords required, and such
  - Called Two-Person Integrity by the DoD

Personnel Security Policies (1)

When we deal with the various types of personnel security policies, it is important to realize that they do not actually prevent anything. Instead, we are attempting to force collusion, making two or more people work together to perpetrate a fraud.

Separation of Duties

No one person has control of a critical process from beginning to end. The classic example is the person who creates invoices cannot pay invoices. If one person can do both, they can potentially generate an invoice for themselves and pay themselves.

Dual Control

No one person can access information alone; it takes two people. This can be implemented by putting two locks on a door to a room (each person can have only one key) or two combinations on a safe (each person can know only one combination). In software, you can require two separate passwords to access data (each person can know only one). This is most commonly found in high-security DoD circles, where it is called Two-Person Integrity.

Personnel Security Policies (2)

- **Job rotation**:
  - For critical functions (payroll, accounts payable, and system admin)
  - Rotate other employees through the function periodically
  - The new person detects that the payroll expert is writing himself five paychecks a month
  - WARNING: Can cause *terrible* political infighting
- **Mandatory vacations**:
  - Critical employees (payroll, A/P) must take a minimum one contiguous week of no-notice vacation each year
  - While they are gone, audit the function
  - They can't cover their tracks while gone

Personnel Security Policies (2)

Job Rotation

For critical functions (especially those dealing with money), you periodically rotate someone else through the position. Although the new person performs those duties, they hopefully become aware of any fraud and report it.

Mandatory Vacations

Certain employees are required to take one additional contiguous week of vacation per year. While they are gone, you audit their function, looking for signs of fraud. Because they are not there, it is more difficult to cover their tracks. This is again most common for those in critical positions handling large sums of money.

Personnel Security Policies (3)

- **Reference check:**
  - Resume: A combination of fictionalized fact and factualized fiction
- **Credential check:**
  - Does this person actually hold a college degree or GIAC GISF certification?
- **Background checks:**
  - A basic records check—do they have 200 parking tickets? (under $10)
  - All the way to a complete 25+ year investigation (expensive)

Every case of espionage against the United States was done by someone with an extensive background check and sometimes even a polygraph.

Personnel Security Policies (3)

Reference Check

Never forget that a resume is a combination of fictionalized fact and factualized fiction. There is a real need to verify information on references. This is especially true for people who will work in highly sensitive positions, including those handling money, and system and network administrators.

Credential Check

Does this individual actually hold that college degree? Or that GIAC GISF certification?

Background Checks

These are important for anyone who will be placed in a sensitive position. They can help you filter certain people out of the process. You do not want someone with a gambling problem and large debt to loan sharks to be put in charge of your accounts payable. So yes, background checks are a good thing. But you should also note that almost everyone who has committed espionage in the last many years HAD a background check. Without it, they would not have had the access to the information they used to hurt us. So, do perform background checks. But also continue to monitor those in sensitive positions. (We say, "almost everyone" because sometimes spouses who have not had background checks are also targeted by foreign intelligence.)

To prove the point that resumes are less than reliable …

- 78% of resumes are misleading
- 21% falsely list a college degree
- 29% show altered employment dates
- 40% have inflated salary claims
- 33% have inaccurate job descriptions
- 27% give falsified references

Reference

http://www.statisticbrain.com/resume-falsification-statistics/

Personnel Security Policies (4): Human Resources and Security

- Getting the security program tied to HR is difficult:
  - HR is used to treating matters privately
- Non-Disclosure Agreement (NDA):
  - Legal document stating an employee will not tell company secrets to competitors
- Employee disciplinary actions:
  - IT Security needs to be informed of formal reprimands
  - Indicates a disgruntled employee—a huge insider threat
- Notification of employee terminations! (Cyber & Physical Security)
  - If they were admin, immediately audit for backdoors and logic bombs

Personnel Security Policies (4): Human Resources and Security

It is difficult to get the security program tied into the Human Resources department, but it is also important. HR personnel are told from the day they are hired they will deal with sensitive information. They are forbidden to talk about hirings, firings, promotions, demotions, reprimands, and more.

Now you, the security professional, waltz into the HR department and ask to be notified of reprimands and firings. It goes against its grain.

One of the greatest threats we face is the disgruntled internal employee. Knowing about disciplinary actions (preferably before the employees themselves) can go a long way toward allowing the security program to curb that threat.

The security staff should also be immediately notified of employee terminations. It is vital that both logical and physical access is terminated as soon as possible.

https://www.wired.com/2009/01/fannie/

Module 4: Authentication, Authorization, and Accountability (AAA)

- Access Control Foundations
- Authentication
  - Something you know
  - Something you have
  - Something you are
- Authorization
  - Access control models
- Accountability
  - Logging and auditing

COURSE ROADMAP

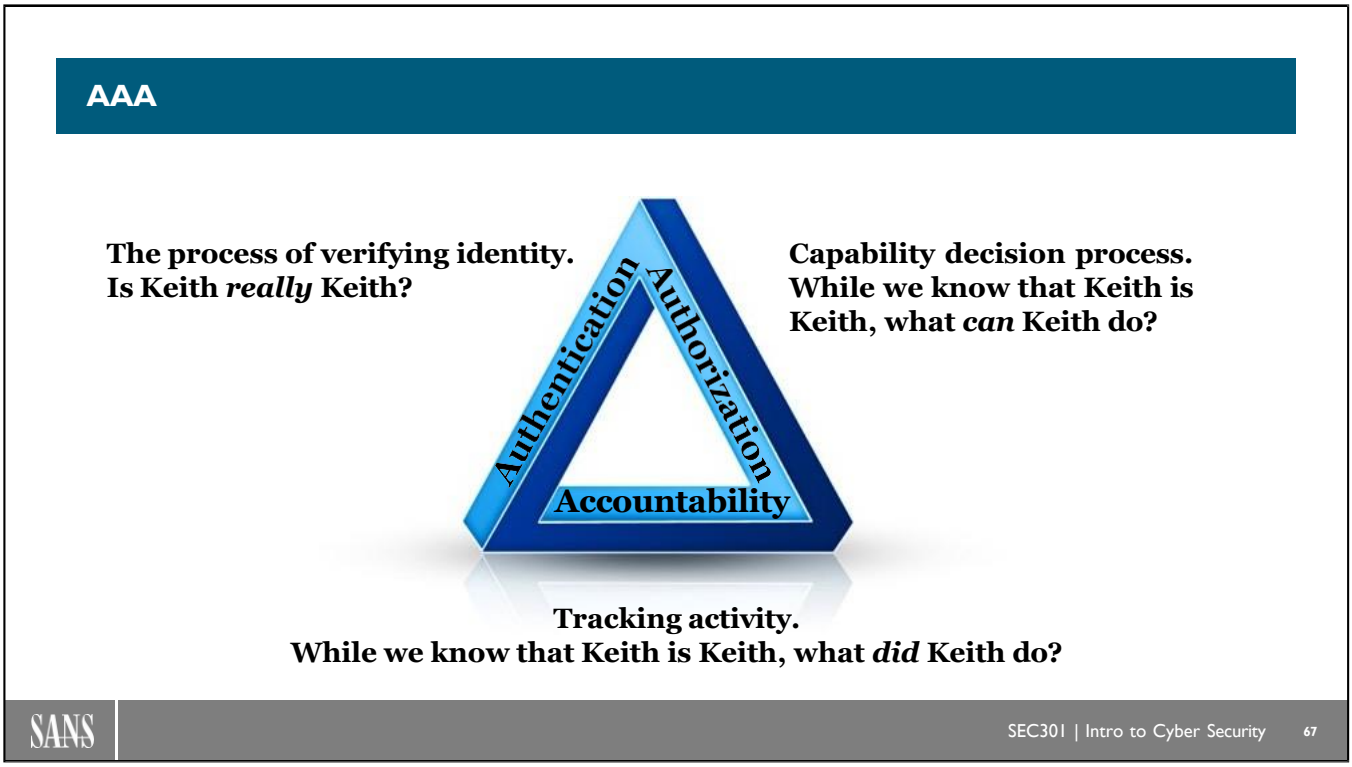
- Module 1: Core Principles
  - Lab 1.1: Introduction to LODS and Quizzes
- Module 2: Risk Management
- Module 3: Security Policy
- **Module 4: Authentication, Authorization, and Accountability (AAA)**
  - Lab 1.2: Building Better Passwords: The Haystack

Module 4: Authentication, Authorization, Accountability (AAA)

Another essential part of any security program is the area of Authentication, Authorization, and Accountability. This is often referred to as AAA.

In this module, we cover:

- Access Control Foundations
- Authentication
  - Something you know/have/are
  - Centralized/decentralized
  - Single sign-on
- Authorization
  - Access control models
- Accountability
  - Logging and auditing



AAA

Authentication

The process of verifying someone's identity. You have an individual claiming to be Keith. You need to know if that person really is Keith.

Everyone knows we have to authenticate users. It's obvious! But few people ever stop to think about why we need to authenticate people. Think it through: Why do you *really* care if Keith is Keith?

Authorization

This is a capability decision process. Although we know that Keith is Keith, what *can* Keith do?

Accountability

This process tracks activity. Although we know that Keith is Keith, what *did* Keith do?

Authorization and accountability are the answer to the preceding question about "Why authenticate?" If we do not authenticate the user, we have no possibility of enforcing authorization or doing accountability. That is why we go through the pain and suffering of the authentication process.

Need to Know versus Least Privilege

- Need to Know = Read Access:
  - If someone needs to know something to do their job, they should be able to read that information
- Least privilege = Capability:
  - If someone needs to *do* something to do their job, they must be able to do it
    - Need to know is a subset of least privilege
- These principles and CIA guide access control decisions:
  - All access control systems should operate on implicit denial
  - Meaning: No access unless explicitly granted

Need to Know Versus Least Privilege

Many people use these two terms interchangeably. There is actually a distinction between them.

Need to Know is about read access. If you need to *read something* to do your job, you should be able to read it.

Least Privilege is capability-based. If you need to *do something* to do your job, you should be able to do it.

Of the two, Least Privilege is the broader in scope. Least Privilege encompasses Need to Know. If you need to have the ability to edit a document (Least Privilege), you also need to read the document (Need to Know).

When you take these Principles of Need to Know and Least Privilege together with the CIA, they guide every decision you make in the access control.

Controlling the Insider Threat

- One of the biggest threats to any organization is the insider:
  - Whether it is the disgruntled insider, the accidental insider, or the external insider, it makes no difference
  - They are inside most of our defenses
- AAA helps to counter this threat:
  - If it is done with the Principle of Least Privilege
    - It will also help to counter Ransomware
    - Ransomware can only impact data the user has access to
  - Topics in other course areas help as well:
    - Personal firewalls
    - Departmental firewalls
    - Intrusion Detection Systems/Intrusion Prevention Systems

But what about admins?

Next slide ...

Controlling the Insider Threat

One of the biggest threats to security in any organization is the insider threat. It is also one of the hardest to defend against. Because the insider works for the organization, they have already been given at least some level of access. This is especially dangerous if the insider becomes disgruntled. Feelings of entitlement often lead to that disgruntlement.

AAA helps to counter this threat in a big way, provided it is implemented with a healthy dose of "and nothing more" from the Principle of Least Privilege.

But there is one thing here you just have to understand. *Sooner or later, you have to trust somebody*. Given the high degree of access you *must* give to your administrators, there isn't much of Least Privilege's "and nothing more" left. Administrators have complete control and access to the systems they administer.

If system or network administrators become disgruntled and decide to hurt your organization, they can. It is extremely difficult to stop a disgruntled system administrator.

Managing Administrator Access (1)

- Multiple people need administrator capability:
  - You *do not* want only one person to have that access and ability
  - You also *do not* want five people all logging in with Admin/root account; there is no accountability
- Assign all administrators their own account:
  - In Windows, assign two accounts: One admin and one non-privileged
    - They then use *run as admin* or *sudo* to perform admin functions
    - All use of these functions should be logged
      - This provides a level of accountability for who performed which action

Managing Administrator Access (1)

Because of the power of the system and network administrators, special considerations need to be given to this level of access. This is especially true on critical servers.

It is necessary for more than one person to have administrative ability on servers. You do not want only one person to have that access in case something bad happens to that person. You need backups for your people as well as for your data.

You also do not want five people all logging in to the Administrator account on Windows or the Root account on UNIX/Linux. If that is happening, you have no accountability for your administrators. If one of them does something bad, you have no way of knowing which of them did so.

Address this by giving all administrators their own non-privileged account (in Windows, you give them two accounts: One admin and one non-privileged). They log in to the non-privileged account, not in to the central administrator or root account. To perform administrative functions, they use *run as admin* on Windows, or *sudo* commands on UNIX and Linux. Because all use of both *run as admin* and *sudo* are logged, this gives you an audit trail to determine which of your administrators did what.

Managing Administrator Access (2)

- Set a *very* strong Admin/root password:
  - Record it on a sheet of paper
  - Seal the paper in an envelope (with tamper markings)
  - Lock the envelope in a safe
  - Nobody logs in with that password, except in the direst emergency:
    - For example: Incident Response

Managing Administrator Access (2)

For the central Administrator account, you need some special protection. Nobody should log in to that account except in the direst emergency.

Set a *very* strong password (35+ characters) on that account. Record the password on a sheet of paper. Seal the paper in an envelope; you can add tamper markings if you want. Lock that envelope in a safe.

Nobody ever logs in to that account, except perhaps during an Incident Response when there is a big problem. The Incident Response team (who may not normally have access to the system at all) suddenly has a valid need for full administrative privilege on the system. Open the envelope and give them the password. When the Incident Response is over, and things are back to normal, change the password and reseal the envelope.

Authentication Factors

- Something you know:
  - Passwords, PIN numbers, cognitive passwords
  - Something you keep in your brain
- Something you have:
  - Tokens, smart cards, and so on
  - Some device you can hold in your hand
- Something you are (or something you do):
  - Fingerprints, retina and iris scans, and more (something you are)
  - Typing dynamics, the way you walk (something you do)
  - This group is called Biometrics
- Somewhere you are (less common):
  - Dial-back modem is a good (but older) example
  - Geolocation/Geofencing is a more modern example
  - Adaptive Authentication (commonly combined with 2-factor)

Authentication Factors

The list of factors you can use to authenticate someone is fairly short. They are listed here, but we cover each in detail as we move through the remainder of this module.

- Something you know
  - Passwords, PIN numbers, and cognitive passwords (such as, "what is your mother's maiden name?") are all examples
  - In other words, something you keep in your brain to prove your identity
- Something you have
  - Handheld tokens, smart cards (CACs in the DoD), and so on
  - These are devices you hold in your hand and use to authenticate in some way
- Something you are (or something you do): Called Biometrics
  - Fingerprints, retina and iris scans, facial recognition (something you are)
  - Typing dynamics, the way you walk, how you sign your name (something you do)
- Somewhere you are (less common)
  - With a dial-back modem, you call the modem and get connected; it hangs up on you and calls you back at a preconfigured number. You have to be at that number to accept the call.

- Geolocation or geofencing is a more modern example. Using a combination of GPS location, Wi-Fi, and Bluetooth, the exact location of a mobile device can be determined. If the device is in the United States, Western Europe, and such, then it is allowed to connect. But if the device is located perhaps in China or Russia, then the connection is denied.
- Adaptive Authentication uses multiple factors of authentication in a dynamic fashion based on criteria at the time of login. For example, when a user is logging in for the first time on a particular device or new computer, the site may ask for a second factor of authentication to raise confidence that they are in fact who they say they are. After the initial login on that device, the system remembers that they logged in from that system. With each subsequent login, they won't need to provide the second factor because they are using a recognized device. Adaptive authentication can include recognition based on an IP address (somewhere you are) component. More commonly, it will use browser cookies (discussed in detail in a later module). In either case, this will help to protect against things like phishing attacks. If a login attempt is coming from the same device (based on IP), or better yet the same browser (based on cookie), there is a high likelihood the user on the keyboard is the same one verified earlier.

SEC301.1 | Introduction to Cyber Security

SANS

Something You Know: General Issues

- Passwords
- Password Issues
- Password Cracking
- Cognitive Passwords
- The Derivative Passphrase
- The True Passphrase

Per the 2021 Verizon Data Breach Investigations Report (DBIR):

87% of hacking-related breaches in 2018 leveraged a password.

Authentication: Something You Know

Every year, Verizon publishes the "Verizon Data Breach Incident Report (DBIR). It normally comes out around April or May. The report examines several thousand breaches from the prior year (e.g. the 2021 report covers breaches from 2018) and reports on the type of attacks used, the cost per record breached, and so on. The information in this report in invaluable when you go to justify security expenditures etc. For example, you no longer have to just guess at the cost per record breached – you now have solid data to base those estimates on.

The Verizon Data Breach Investigations Report (DBIR) can be downloaded from:
https://enterprise.verizon.com/resources/reports/dbir/

Something You Know: General

- Anything you must remember to authenticate:
  - Passwords, PIN numbers, passphrases, cognitive passwords
  - They are extremely common in everyday life
  - Therefore, people think they understand the issues with them
    - They are wrong … especially security people!

- Often touted as inexpensive:
  - Passwords are built into the system; nothing extra to buy
  - Not inexpensive when you add user training, help desk time unlocking accounts, lost productivity due to locked accounts, and so on

Something You Know: General

As stated earlier, something-you-know authentication is anything you store in your brain and must remember to authenticate. This is, without question, the most common form of authentication.

Unfortunately, passwords are so common that people (especially security professionals) assume they understand them well enough and give them little or no thought. This is a primary contributing factor to why we have had so many problems with passwords over the years. This next section will try to remedy that for you.

Because passwords are built into the system, this form of authentication is often touted as inexpensive. You don't have to pay extra to add passwords. You should always look at the total cost of ownership (TCO) for everything.

The reality is that something-you-know authentication can cost you more than you realize. When you add in user training on choosing good passwords, help desk time unlocking accounts, lost productivity due to locked accounts, and so on, the costs add up quickly. On an annualized basis, passwords are actually expensive. (When you look at the time spent managing passwords; remember our example earlier of inappropriate web surfing and the weighted rate for employees.)

Passwords (1)

- Good passwords consist of uppercase/lowercase/ special characters/numbers
- Longer passwords are better passwords:
  - Increases the “password universe” (number of possible passwords)
  - Helps against brute force
- NIST SP 800-63B (June 2017)
  - Forget complexity
  - Focus on length and use password managers
  - Only do password resets if there is a compromise or a request
    - Requires monitoring successful logins

Passwords (1)

Everybody has gotten this training at least once in their career. Good passwords consist of uppercase, lowercase, special characters, and numbers; longer 15-character passwords are better than shorter 8-character ones.

The length of the password is indeed an important issue. The longer the password, the larger the "password universe." This is a fancy way of saying how many possible passwords you can create given the allowed character sets and the number of positions. Make no mistake: Longer passwords are decidedly more secure than shorter ones. (Password universe is an almost identical concept to *keyspace*, which we discuss in the cryptography section.)

IT Security practitioners have given the same bad advice to the user community for more than 40 years. That advice amounts to, "If you can remember a password, it is a bad password." Or to say it another way; “If it is possible to actually *use* a password to authenticate, you are doing it wrong.” This is bad advice.

Unfortunately, the standard advice saying to use uppercase, lowercase, special characters, and numbers plus longer is better leads to a problem. The impossible-to-remember password! We (the IT Security community) have to fix this problem and start explaining to users how to create strong passwords that can be remembered and easily typed into the system. By the end of our discussions here, you will understand how this is possible and be prepared to pass that advice along to others.

Passwords (2)

- Maximum and Minimum password aging:
  - Maximum = You must change password every X number of days
  - Minimum = Cannot change password more than once a day
- Password histories:
  - Remember the last 10 passwords to stop reuse
- Password strength checkers:
  - Ensure upper, lower, special, number

Passwords (2)

You need to understand several terms surrounding password security. Here we look at some of them. We will take them slightly out of order from what you might expect, but you will understand why in the end.

Maximum Password Aging

This setting requires you to change your password every 60 days or every 90 days. The purpose behind this setting is that if your password is compromised, the window of opportunity for someone to use that password is smaller. Also, it is hoped that you change your password before someone is successful in compromising it via a password cracking attack.

Password Histories

This setting causes the system to remember the last X number of passwords. You cannot then reuse that particular password for "X" amount of times of changing your password. For example, let's say this setting is at 10 and you currently have a password of Rover1#. The maximum aging setting tells you it is time to change your password. You cannot change your password from Rover1# *to* Rover1#. In fact, you would not be able to use Rover1# as your password again for the next 10 passwords in this example.

As you will see, these can be combined with password strength checkers as well.

Minimum Password Aging

This setting says that if you change your password today, you cannot change it again for one day (Or sometimes you will see five days for this setting). Why would we want to put that restriction in place?

We have actually seen it happen. The password history says you cannot reuse the last five passwords. Maximum aging says you must change your password today. So, you change your password to five random passwords, and on the sixth, you set it back to what it was to begin with, all in one sitting. Minimum aging is designed to prevent this type of foolishness.

Password Strength Checkers

These can ensure that you have, for example, at least one uppercase character, one lowercase character, one special character, and one number in your password. That is probably the most common usage, but it is not all they can do.

Some organizations combine the password history with the strength checker. Let's return to our example of the password Rover1#. When you put the history list together with the strength checker, it would be possible to prevent you from using Rover2# or similar. Some will implement this in such a way that you cannot repeat any three characters of a password in the history list. So, none of your next five passwords could contain *ove* because that string is contained in Rover1# in the history list.

Some will also implement strength checkers to say you cannot have any three like characters in a row. This would mean you cannot have three lowercase in a row for example. That would extend to any three uppercase, special characters, or numbers in a row as well.

Exercise caution with strength checkers and password histories. If you configure your system to remember the last 100 passwords, any new password cannot repeat any 2 characters from the history; no two repeating characters are allowed; all passwords must begin with a two-digit number; all passwords must contain 3 uppercase, 3 lowercase, 3 special characters, and 3 numbers and must be at least 20 characters in length; and they must be changed every 30 days. That sounds ridiculously complex and it is—that is our point—it is ridiculous. Not only will you have a user revolt on your hands, you also will soon face a situation in which no user can choose a new password.

Incidentally, in **NO WAY** is any of this text intended to indicate that Rover1# is a good password. It is not. We simply needed a string to use as an example.

Passwords (3)

- Account Lockout: e.g. three bad passwords, lock the account
  - Lockout duration: 120 minutes
  - Reset counter after 45 minutes or successful login
  - Beware of Denial of Service (DoS) potential

- Originally to stop the keyboard brute force
  - Those cannot work against longer (15 character) passwords
- Could be for ID'ing automated brute force:
  - Set lockout at 100
  - Generate alarms if that is reached

Passwords (3)

The account lockout policy is an old favorite for password security settings. It has been around a long time. This is the setting that says if you enter your password wrong, say three times, your account will lock for a period of time. (Note: The number three is the most common setting, but you will often see five used for account lockout as well.)

When putting these settings in place, there are some things you need to take into consideration, such as the lockout threshold (called a *clipping level*). What is the correct number of bad passwords after which you need to lock the account?

The recommendation for this setting has changed over the years. Understand that when account lockout was first invented in the 1970s, the longest password allowed by the system was only eight characters and passwords of four or five characters were normal. In those days, there was a potential for someone to sit at the keyboard and enter possible passwords until one worked … the keyboard brute-force attack.

Today, organizations regularly require longer passwords. Fifteen-character minimums are not uncommon. The keyboard brute-force attack is nonviable against a password that long. Instead, today this setting should be used for identifying the automated brute-force attack, software launching many login attempts using different passwords from a dictionary.

In that case, you can set the threshold much higher, say 50 or even 100, and then ensure an alert and/or alarm is generated as soon as that threshold is hit. This should immediately lead to an investigation.

Password Issues

- People choose passwords that are easy to remember:
  - Easy to remember = easy to guess (See Next Slide!!!)
- Password reuse is common:
  - Is your email password also your PC password?
  - How many websites do you use the same password on???
- They often have repudiation issues:
  - Sticky note on a monitor: Prove someone else didn't put inappropriate material on their computer—you can't
- People write them down!!!
  - We all know that is bad, don't we?!
  - Actually, a good password manager is recommended

Password Issues

Password security is not all about technology. It is also about human nature. One of the problems we face with passwords is that people want and need to choose passwords that are easy to remember. Unfortunately, passwords that are easy to remember are also usually easy to guess. Again, this does not have to be true, as you will see, but it often is.

Another part of the human nature issue is that when someone comes up with what they think is a strong password, they reuse that password on many different sites.

A common industry best practice is to never write your passwords down. If you are putting them on a sticky note on the monitor or under the keyboard, we agree. However, we actually recommend the use of a good password manager. This is software that will keep all your username and password information in a passphrase-protected encrypted file. With proper implementation, this can enhance your personal security a great deal.

https://www.splashdata.com/worstpasswords

10 Most Common Passwords Found In Internet Breaches

Rank	2011	2012	2013	2014	2015	2016	2017	2018
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou	iloveyou

Only 5 have more than one character set…

List of top 25 @ https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#SplashData

10 Most Common Passwords Found In Internet Breaches

Every January, Splashdata publishes the most common passwords from the prior year. The data is based on the passwords discovered during an internet breach. For example, if a website has its passwords published online, they then become included in the Splashdata report.

Above is the Splashdata information on the 10 most common passwords from 2011 to 2018. It paints a pretty sad story. Especially when you notice that only 5 of the passwords on the list use more than one character set – and none of them did since 2013! Many complain that the https://www.grc.com/haystack site that you will use in your upcoming lab assumes the attacker knows the character set used by the victim. This slide plainly illustrates why the attacker usually does know the character set.

You can get the full list of the 25 most common passwords since 2013 at:
https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#SplashData

Each year, you can find the full list of the 100 worst passwords at:
https://www.splashdata.com/worstpasswords

Password Cracking (1)

- Software that cracks (or guesses) passwords
- Can be used by admins and attackers:
  - Without written permission, it is illegal in the U.S.
- Commercial password crackers:
  - L0phtcrack: Decent
- Free password crackers:
  - Offline:
    - John the Ripper: http://www.openwall.com/john/
    - Hashcat: http://hashcat.net/ – Very Fast!
    - Cain and Abel
  - Online
    - THC-Hydra: http://sectools.org/tool/hydra/
  - Most perform dictionary, brute force, and other attacks

Many countries have different laws regarding possession and use of "hacking tools."
See notes …

Password Cracking (1)

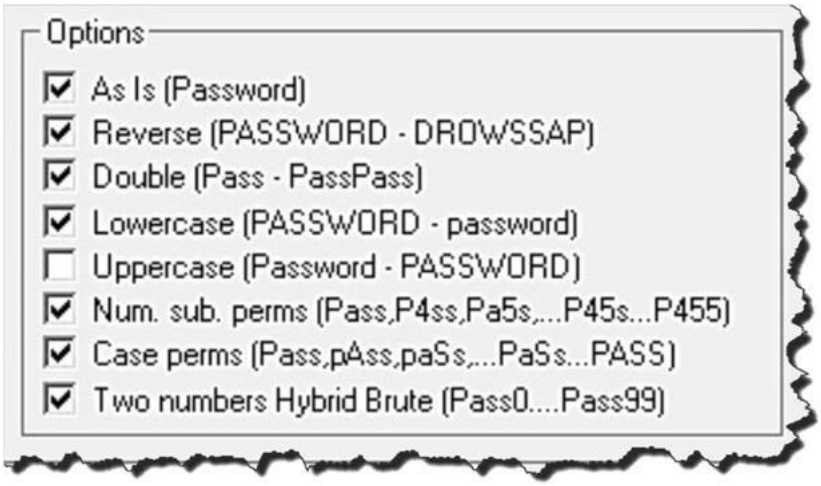
Several password crackers (software) are available. A few are commercial that you pay for. Most are open source and therefore free. Administrators will sometimes use password-cracking software to recover a password for a user. However, it is more common to simply change the user's password.

The most common use of this type of software is by attackers who use it to crack passwords of victims. This type of software usually falls into two categories: The offline password cracker and the online brute forcer.

The offline password cracker, such as John the Ripper, Hashcat, or Cain and Abel, work offline, meaning attackers obtain your password file by some means (often some sort of an exploit). They have that file on their computer and are attempting the password attack there, which means your account lockout settings have no impact. The other common type is the online brute force software, such as Brutus, iBrutus, and Hydra. These work by attempting to log in to an account repeatedly, typically using different passwords from a dictionary.

NOTE: Even if you are a system or network administrator, if you do not have specific written permission to use these types of tools in the United States, it is illegal to use them. Within the EU member states, there is often a disjointed approach, with each country often having different laws with some far more robust than others, e.g. Germany. The EU GDPR is seen by all member states as a real step in the right direction and its principles will almost certainly need to be adopted even by the non-EU countries that wish to do business in the EU or with EU citizens.

Password Cracking (2): Dictionary "Word Mangling" Rules



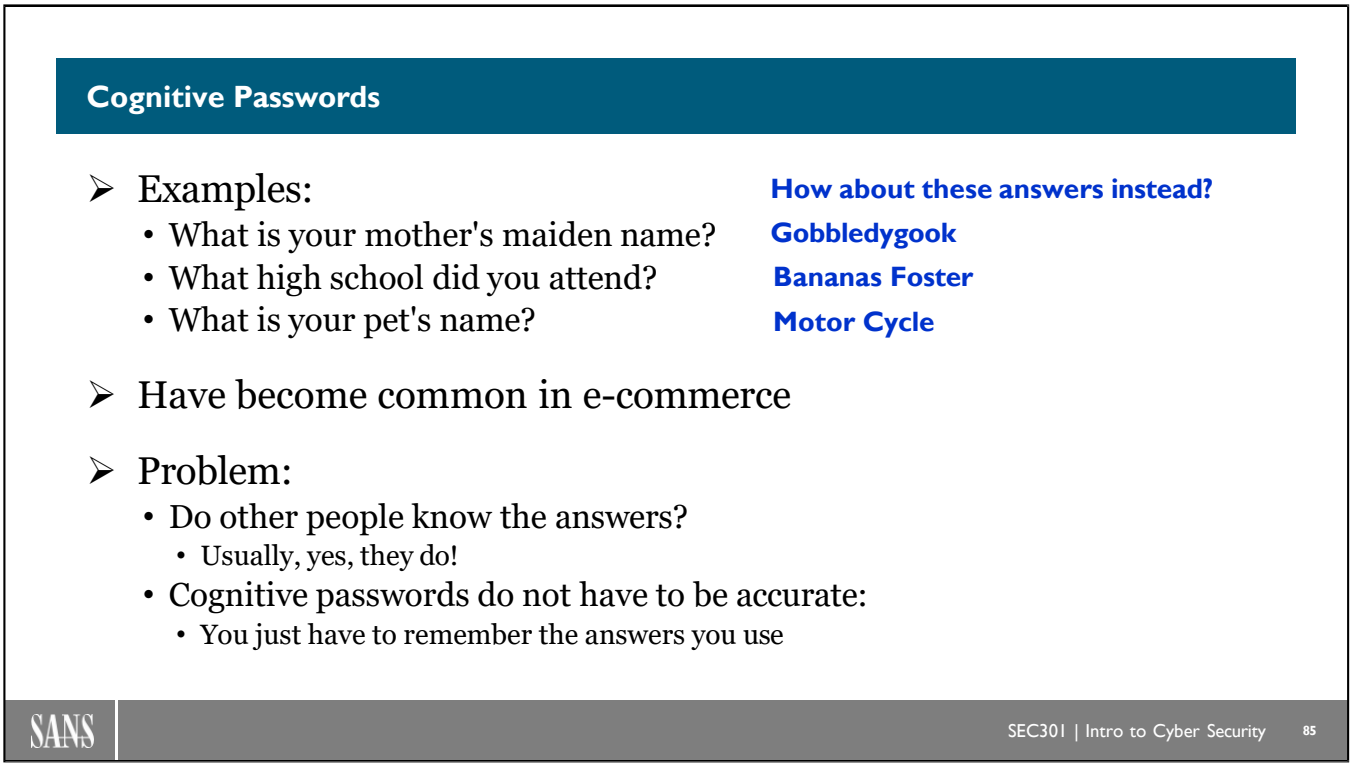
Password Cracking (2):
Dictionary "Word Mangling" Rules

Most password-cracking software includes the ability to use mangling rules on words from a dictionary. Meaning they take a word from a dictionary and mangle it or modify it in specific ways. In this slide, you see a screenshot from Cain and Abel, one of the few graphical password crackers. In the screen you see here, you can select the mangling rules you would like to use.

- **As is (Password):** Checks the dictionary word as it is in the dictionary.
- **Reversed (PASSWORD – DROWSSAP):** Reverses the letters of the dictionary word.
- **Doubled (Pass – PassPass):** Causes the dictionary word to be doubled before checking.
- **Lowercase (PASSWORD – password):** Forces the dictionary word to all lowercase characters.
- **Uppercase (Password – PASSWORD):** Forces the dictionary word to all uppercase characters.
- **Num. sub. perms (Pass,P4ss,Pa5s,…P45s…P455):** Short for "Number Substitutions Permutations" causes the substitution of certain numbers with certain letters. For example, a's are replaced with 4's, and s's are replaced with 5's. It does these substitutions in every possible combination.

- **Case perms (Pass,pAss,paSs,…PaSs…Pass):** Short for *Case Permutations*, causes the dictionary word to be tested in every possible combination of capitalization.
- **Two Numbers Hybrid Brute (Pass0…Pass99):** Appends up to two numeric digits after each dictionary word. (John the Ripper also appends special characters like ! and #.)

The next time you select a password, you might keep these rules in mind and avoid dictionary words as well as the mangled forms of dictionary words. It should also be noted that some password crackers, such as John the Ripper do far more "mangling" of words from a dictionary than what is shown here. In fact, John the Ripper has over 1,700 total mangling rules by default.



Cognitive Passwords

These have become extremely common, especially in e-commerce and online banking. Typically, a site asks you a question such as "What is your mother's maiden name?" and records your answer. At a later point, if you need to change your password or if you are accessing its system from a computer it doesn't recognize, it asks the question again. You have to give the correct answer.

The problem with cognitive passwords is that other people know the answers to these types of questions. For many people, there is one person they *don't* want in their bank account but can answer every cognitive password correctly—specifically their ex-spouse. In another example, if you stand on your back porch and call your dog, do you think your neighbor knows your pet's name?

The answers you provide to cognitive passwords do not have to be accurate. You just have to remember them. For years, the author used information from the movie *Grease* to answer cognitive password questions. His mother's maiden name was Newton-John, he attended Rydell High, and his pet's name was Travolta. (How dare he date my girlfriend Olivia!) None of which was accurate, but all of which was easy to remember.

The Derivative Passphrase

- You can create effective passwords this way …
- You can often generate passphrases on-the-fly:

LMMs0aT~Tcj0tM2

- **Little Miss Muffet sat (zero) on a Tuffet (while) ~ The cow jumped (zero) over the Moon Twice (two)**
- It has uppercase, lowercase, a special character, and numbers
- **But these tend to be hard to remember and type!**

The Derivative Passphrase

Many people recommend that you create what they call a passphrase but what is actually more accurately a derivative passphrase. The one you see on this slide is an excellent example. Although this is indeed a good passphrase that would stand up well to a password attack, there is a problem with this method. How many websites do you need to log in to? Can you come up with something of this nature for every one of them? Remember you need a different password on every website.

There is a better way …

True Passphrase

- Instead of taking a letter from the start of each word as with the derivative passphrase
- Why not just use the phrase itself?
  - Most websites don't allow spaces, so …
  - The 20 character: WhatdoestheFoxsay?18
  - 11.52 thousand trillion centuries of protection against the fastest password attack today:
    - By contrast, LMMs0aT~Tcj0tM2 from the last slide gives 1.49 million centuries

If you *can* use spaces, do so …
The password "What does the Fox say? 18" provides 89.14 trillion trillion centuries of protection.

True Passphrase

You don't have to use the derivative method to create a passphrase. Instead of taking certain letters from a given phrase, why not just use the phrase itself? When you do this, remember that many websites will not allow for spaces in passwords. So simply type the phrase without spaces. Add some punctuation and some numbers that make sense.

For example: WhatdoestheFoxsay?18

This is the title of a popular (if highly annoying) song. It is easy to remember and easy to type. The 18 on the end comes from the fact the string "WhatdoestheFoxsay?" is 18 characters long.

Note: Most websites and some operating systems do not allow for spaces in passphrases. If the site or system you use does allow for spaces, by all means, use them.

When we enter that passphrase at the website: http://www.grc.com/haystack, we find that even against the fastest password attack possible today, it still provides 11.52 thousand trillion centuries of protection (more than 11.5 Quadrillion years, or 11.5 Billard years in European terminology).

You will have an opportunity to work with the grc.com/haystack site in the lab today.

Lab Time

- LAB 1.2: Building Better Passwords—The Haystack
- Objectives:
  - Use LODS to access this tool
  - Use a tool to determine how long it would take to *brute force* a password
  - Estimated completion time: 25 minutes

Find this utility online at: https://www.grc.com/haystack.htm

Lab Time
LAB 1.2: Building Better Passwords—The Haystack

This tool is found online at https://www.grc.com/haystack.htm

Similar tools are available at the links below. We don't like them as well as the Haystack tool you use here, but you can check them out to determine your preference.

http://password-checker.online-domain-tools.com/
https://www.betterbuys.com/estimating-password-cracking-times/
https://howsecureismypassword.net/

Token Authentication Introduction
Token Examples
CAC/PIV/Smart Card

Authentication: Something You Have

This page intentionally left blank.

Token Authentication (1)

- A device you hold in your hand
- Three general categories:
  - Synchronous: Time-based
  - Asynchronous: Challenge/Response
  - Possession-based: Proximity
- Issues with all:
  - Loss may permit use
  - Susceptible to breakage, dead batteries, and so on
  - You must have them with you to use them

Token Authentication (1)

Something you have, or *token-based authentication*, is some type of device you hold in your hand. Most commonly, some type of small token or smart card. Let's now look at examples.

Following are three general categories of token-based systems:

- **Synchronous:** Time-based systems
- **Asynchronous:** Challenge/response systems
- **Possession-based:** Proximity systems

With any token-based system, there are potential issues. You must have them in your possession to use them. (They don't do you much good sitting on the nightstand at home.) In much the same category, there is the possibility of breakage, dead batteries, and such. Unless there are additional protections in place, if you lose the token, someone else may use it. With some (smart cards in particular), you have to have a special reader that is not common on most computers. You can typically use them only at work.

Token Authentication (2)

- Many (possibly all) token-based systems are also …
- **One-Time Password** systems
- Meaning the password can be used once and once only
- Defeats a **replay attack**:
  - Any time your authentication information is captured and reused to authenticate as you

Token Authentication (2)

Many and, in fact, most token-based systems are also One-Time Password Systems. This simply means that whatever password is generated by the token can be used once and never again. It is good one-time only, as the name implies.

This is valuable in defeating something called a Replay Attack. These attacks occur anytime your authentication information is captured and reused by attackers to allow them to authenticate as you. Hence, the name Replay Attack because they replay your authentication information.

With one-time password systems, this type of attack is not possible. Even if the attacker does manage to capture your authentication information, it won't do them any good.

Two-Factor/Dual-Factor/Multifactor Authentication

- Any time you use two or more of something you Know/Have/Are
- Terms are used interchangeably

- So:
  - Systems that require you to know a PIN # and use a token to authenticate are ...?
  - Systems that require you to use a token, your finger, and know your password are ...?
  - Systems that require you to know your username, your password, and a PIN # are ...?

Also called: 2FA and MFA

Two-Factor/Dual-Factor/Multi-Factor Authentication

We know that there are three primary factors for authentication:

- Something you know
- Something you have
- Something you are

When you combine two or more of these together, you have a two-factor authentication system. Assuming proper implementation, using more than one factor for authentication will always make authentication harder to defeat and, therefore, more secure.

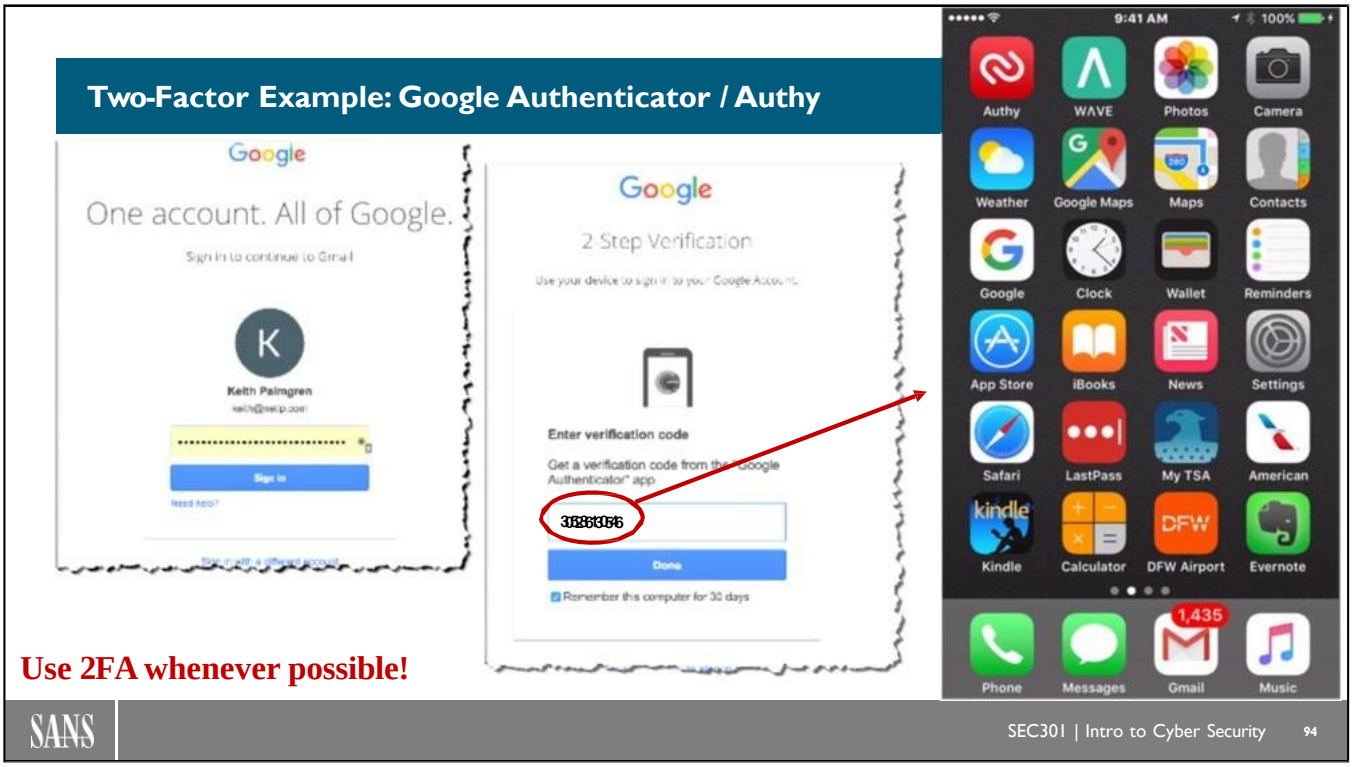
Technically speaking, combining any two factors is two-factor, whereas combining all three is *multifactor*. Having said that, be aware that most people (and vendors) use these terms interchangeably. It is also good to note that some vendors will refer to a two-factor or multifactor authentication system as *2FA or MFA.*

So:

- A system that requires you to know a PIN # and use a token to authenticate is a …?
  Two-factor authentication system
- A system that requires you to use a token, your finger and know your password is a …?
  Multifactor authentication system

- A system that requires you to know your username, your password, and a PIN # is a …?

  Single-factor authentication system. (This is three of one factor, something you know.)



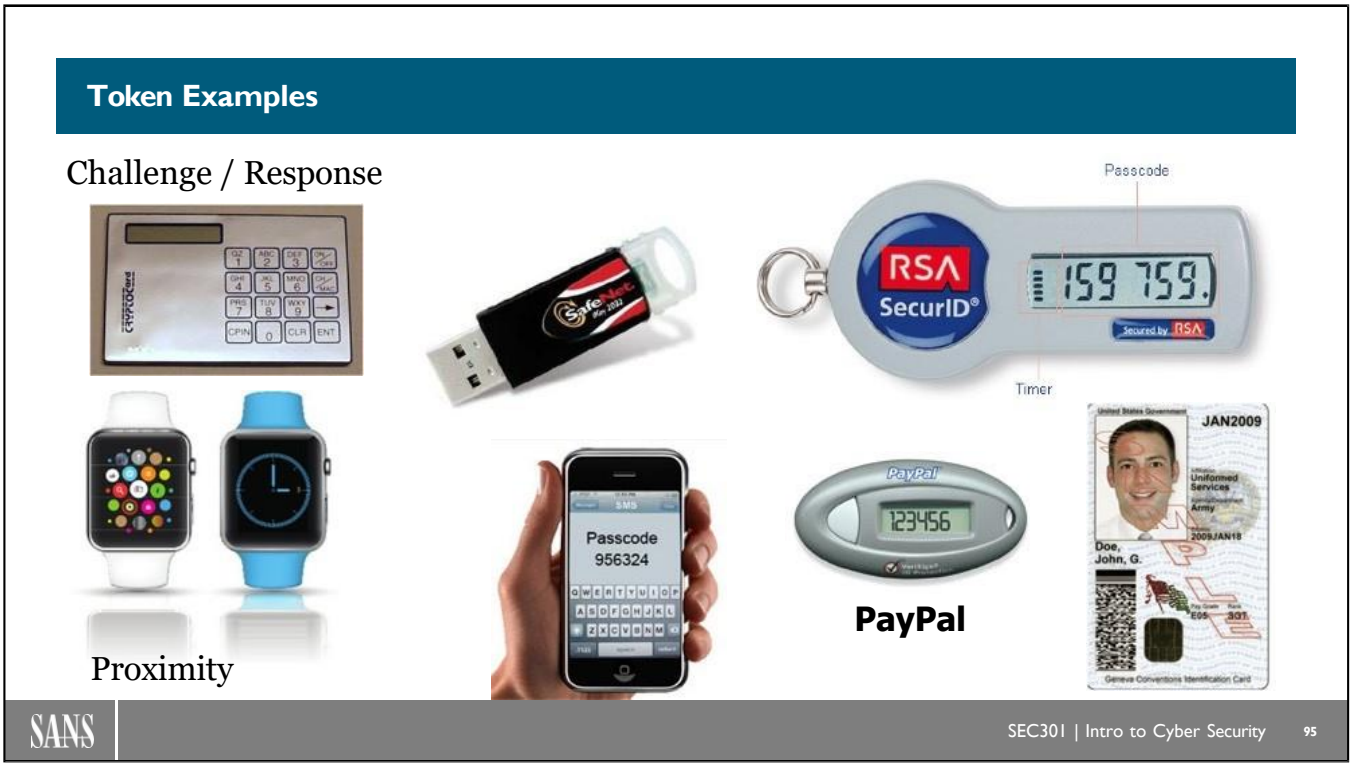
Two-Factor Example: Google Authenticator / Authy

There is a growing trend for some internet sites to offer additional authentication. Gmail, Twitter, LinkedIn, Facebook, and others now have this as an option.

In brief, when you authenticate with your username and password, you then enter an additional one-time code to complete the authentication. You sometimes receive this additional code via a text message. Another popular option is the one you see on the screen called Google Authenticator. Each of the sites you have configured to use this smartphone app is listed and each has a different one-time use code every 30 seconds.

In this way, you have the advantage of two-factor authentication (something you know = your username/password and something you have = your smartphone) as well as a one-time password system. Now, even if people somehow compromise your password, it does them no good unless they also have your smartphone and can access it. Hopefully, you have authentication on your phone as well!

You should *strongly* consider the use of these authentication methods on any and every site you are allowed to use them on. You might also want to consider lobbying your online bank and other such sites to begin offering these methods as an option as well.



Token Examples

Probably the best-known token authentication system today is the RSA SecurID token (upper-right corner on this slide). This is a synchronous system in that it displays a new 6-character numeric password every 60 seconds. It is also a one-time-password system in that the password is only good once. This serves to defeat replay attacks. (There is also typically a 6-digit PIN # that you have to enter to use the SecurID token.)

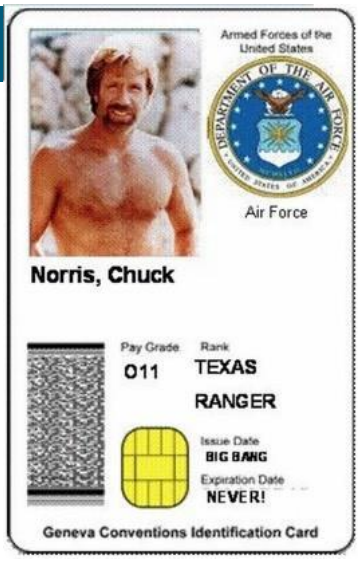
Similar tokens are available from several companies. (Here you see one from PayPal.) You can even use "soft tokens" on a smartphone that work the same way.

The CryptoCard in the upper-left corner is a classic challenge/response token. When you log in, you enter a username & PIN #. The system sends you a numeric challenge. You punch the challenge in on the CryptoCard number pad and then press the ENT key. A response appears on the screen of the device. You type that on your keyboard to authenticate.

Finally, the lower left is an example of a proximity device. In this case, an Apple Watch. If you have a Mac computer (from Apple) and an Apple watch, you can configure the system to unlock anytime you come near wearing the watch. Even once set up, the feature does not work unless you first press a key on the keyboard. Also, you must have entered a four-digit passcode on the watch when you first put it on your wrist. Perform this authentication step before you approach the computer. Once all of that is in place, you can walk up to your Mac computer, hit a button, and start working.

CAC/PIV/Smart Card

- Common Access Card (CAC) and Personal Identification Verification (PIV) Card:
  - Both are a form of Smart Card
  - A card with a chip on it:
    - The chip contains a Certificate (X.509 or similar) used for authentication
- CACs are used by the DoD:
  - PIVs are implemented by other government agencies (for example, NASA)



CAC/PIV/Smart Card

In the United States DoD, every military member and civilian employee carries a Common Access Card or CAC. It looks something like the one of Chuck Norris that you see here. Notice there is a chip in the lower center of the card (which means this is a "smart card"). You place this card into a smart card reader, which reads information off of the chip that is used in authentication. Specifically, in this case, it is reading information from a digital certificate (another topic in cryptography later). In this implementation, the user also has to enter a complex password to unlock the information on the chip.

Some U.S. government agencies have implemented similar but slightly different smart card authentication systems. For example, at NASA, it is not called a CAC; it is instead called a Personal Identification Verification (PIV) card.

There is finally a push in the United States to move to smart card technology for credit cards as well. The United States is the only first-world country that has not already done so. Although this is not a perfect solution (additional protection would be required for *card not present* transactions such as online shopping), it can help a great deal with credit card fraud. Unfortunately, the United States moved to *chip and signature* credit cards instead of *chip and PIN* credit cards. Chip and signature are far less secure.

SEC301.1 | Introduction to Cyber Security

SANS

Biometrics: General Process
Biometric Types
Biometric Examples
Biometric Issues

Authentication: Something You Are

This page intentionally left blank.

Biometrics: General Process

- Registration:
  - User presents biometric to a reader multiple times:
    - No two biometric reads will be identical
  - System takes best average, creates a *biometric template*:
    - Stores template with username
    - May be hashed, encrypted, and more … or not
- Usage:
  - User enters a username
  - System grabs the associated template
  - User presents biometric to the reader
  - Read and template are compared
  - They WILL NOT match; it is a question of "are they close enough"

Biometrics: General Process

Moving into a discussion of *something you are* authentication takes us to biometrics. These have actually been around since at least the late 1980s in one form or another. However, it is just in the last few years that their popularity has started to take off.

Regardless of the type of biometric system you are going to use, there is a standard process you follow. First, you present your biometric (such as a fingerprint) to the system anywhere from 2 to 10 times. The system takes the best average of those reads and creates a biometric template and stores it with your username.

Later, when you log in, you present your biometric to the system. It compares that read to the template stored on the system. Because no two biometric reads are ever identical, it will not be an exact match. It has to be a *close enough* match.

There is a threshold you have to set: Does it need to be an 80% match or a 90% match? Getting that threshold right is the secret to success with biometrics. Too high and nobody can authenticate to the system. Too low, and anybody can authenticate, even if they shouldn't be able to.

Biometric Types

- Something you *are*
  - Fingerprint
  - Iris Scanning
  - Retina Scanning
  - Face Recognition
  - Hand Geometry
  - Voice Recognition
- Something you *do*
  - Keyboard Typing Dynamics
  - Biometric Signature
  - The Way You Walk
- None of "Something you do" methods are very accurate

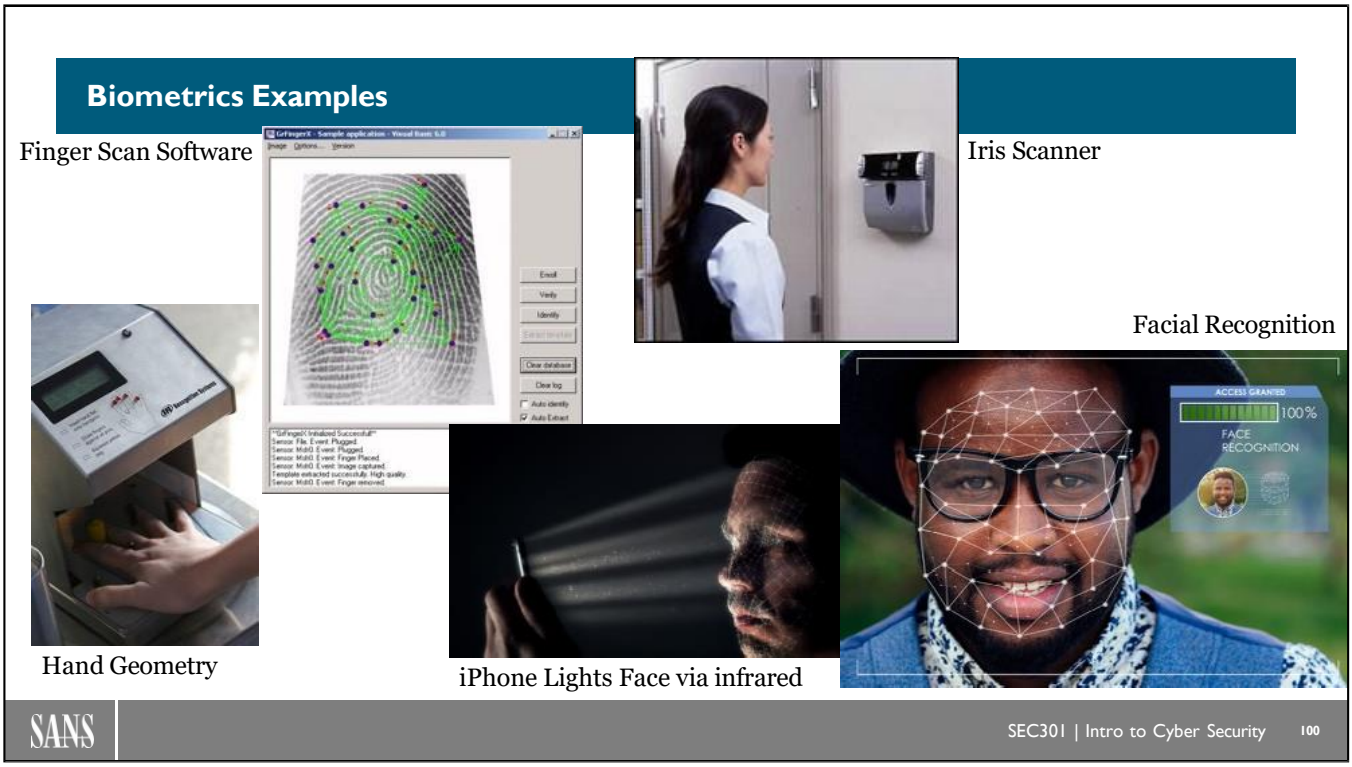
SANS SEC301 | Intro to Cyber Security 99

Biometric Types

As you can see here, several types of biometric systems are available. On the left are the *something you are* types, and on the right are the *something you do* types. The something you are biometric systems tend to be better.

Almost certainly, fingerprint biometrics is the most common today. After that in popularity is probably facial recognition, followed by iris scan.

Each has its good points and bad points. Some lend themselves better to certain situations than others. Choosing the best biometric system for any given situation requires research.



Biometrics Examples

Here are several examples of biometric systems. In the finger scan software example, you can see the system does not actually store your fingerprint. Instead, it looks at measurements between points on the finger. Facial recognition works similarly. It is not a picture of your face; it is measuring the distance between points.

Biometrics Issues

- Acceptance
- Accuracy
- Effectiveness
- Attacks

- Two Important Firsts:
  - Authentication NOT based on a secret
  - Security mechanism that is also a convenience devi ce

- The ROI model makes sense:
  - They can pay for themselves over time
  - Even compared to those "inexpensive" passwords

Biometrics Issues

Regardless of the type of system you choose, you need to be aware of certain issues.

Do not disregard the question of user acceptance. Many people find biometrics to be intrusive and some consider them to be an invasion of privacy. If you understand the biometric types and how they work, you can usually alleviate these issues.

Each of the different types has varying degrees of accuracy and effectiveness, often depending on environmental conditions. For example, some use cameras that require consistent light levels to work. Others don't work well in dusty, dirty, or wet environments.

Each biometric type can be attacked. Some vendors are aware of these attacks and go to great lengths to address them. Some vendors do very little. Again, research is required here. (Note: Few attacks in the movies actually work against real-world biometric implementations.)

It is important to note that biometric systems enjoy two firsts in the security world.

1. The first-time authentication is not based on a secret—passwords must be kept secret! The algorithm to generate SecurID token passwords must be kept secret, and so on. Here, your fingerprint or your face is not a secret. With proper implementation, it does not need to be for these systems to remain secure.
2. The first security mechanism that will make a system both more secure AND easier to use—most security makes systems harder to use. Well-implemented biometrics are easy to use and provide a decidedly better level of security than passwords.

SANS

Subjects and Objects
Access Control Models
➢ (DAC/RBAC)

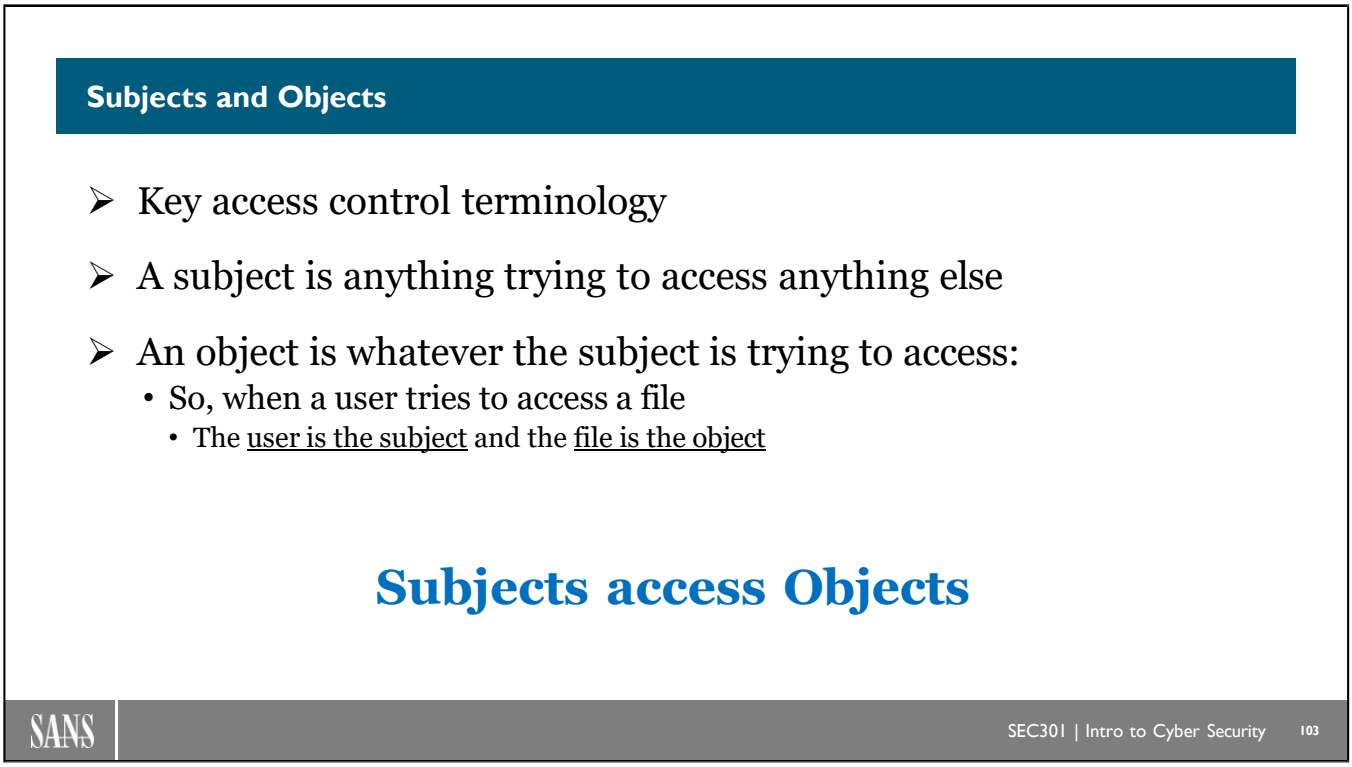
Authorization

Authorization

Now that we know how to confirm identity with authentication, we are ready to move on to authorization. What will you allow that confirmed identity to do on the system?

In this area, we cover:

- Subjects and Objects
- Access Control Models
  - (DAC/RBAC)



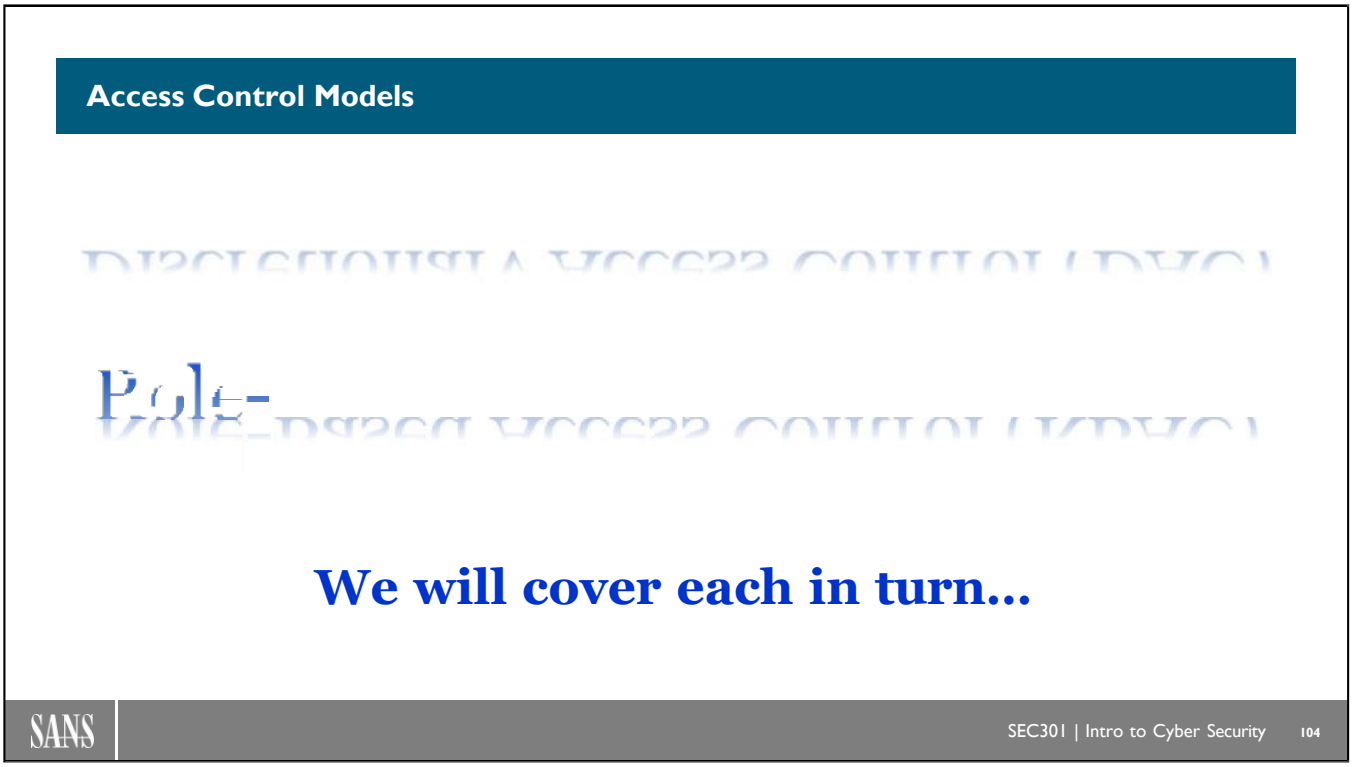
Subjects and Objects

Anytime you study the topic of access control or authorization, you see the terms *subject* and *object*. These terms are not difficult, but if you don't know how they are used here, it can become confusing.

Subject: Anything that is trying to access anything else.
Object: Whatever the subject is trying to access.

So, for example, when a user on the system attempts to access a file, the user is the subject and the file is the object. Or when a browser is accessing a web page, the browser is the subject and the web page is the object.

You need to understand these terms because you will often see explanations that include wording such as, "when a subject accesses an object …" or "The system determines if a subject should be able to access an object based on …" The terms are used by many texts on security, but not many of them ever take the time to actually tell you what they mean.



Access Control Models

You can also employ several models for controlling access. Here, you see the two most common listed. We are going to go through each one in turn.

Discretionary Access Controls (DAC)

This is almost certainly what you use at home.

- Default on Windows, UNIX/Linux, Mac
- Every file on a computer has an account assigned as the file's owner
- Owner has the *discretion* to grant access to another user:
  - The file in question has an ACL associated that tracks permissions



File Owner

Owner changes permissions
Grants access to another user
Up to the "owner's discretion"

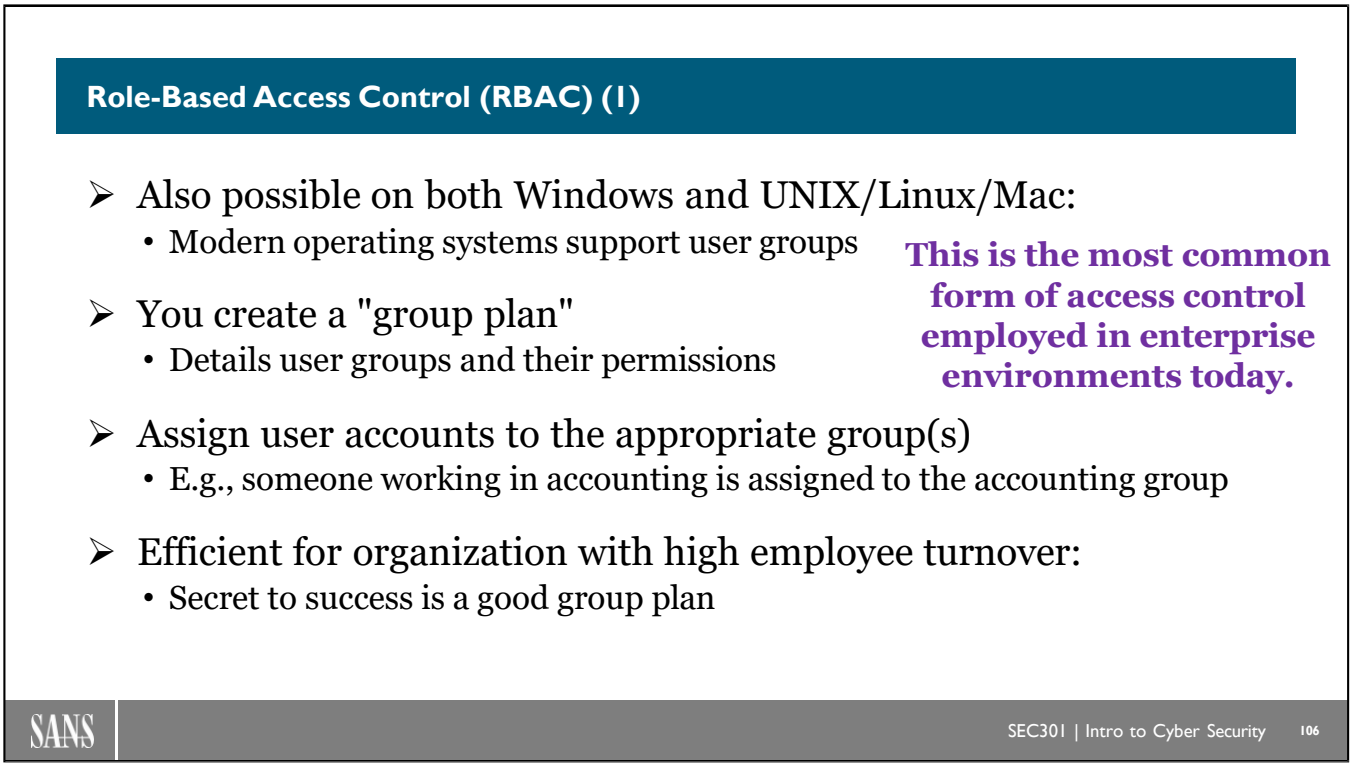
Other User

Discretionary Access Controls (DAC)

The Discretionary Access Control system may be the one you are most familiar with. If you install Windows, UNIX, or Linux and do not set up anything special, this is how they work by default.

In this case, every file and directory have some user account assigned as the file's owner. That user (the owner) can give other users access to the file. The file owner grants that access at their discretion, hence the name Discretionary Access Control.

The mechanics of how the file owner grants that access will vary by operating system type. But generally speaking, the owner of the file will use whatever mechanism is in the OS for changing the file's permissions. The owner changes the file permissions to grant access to another user or users.



Role-Based Access Control (RBAC) 1

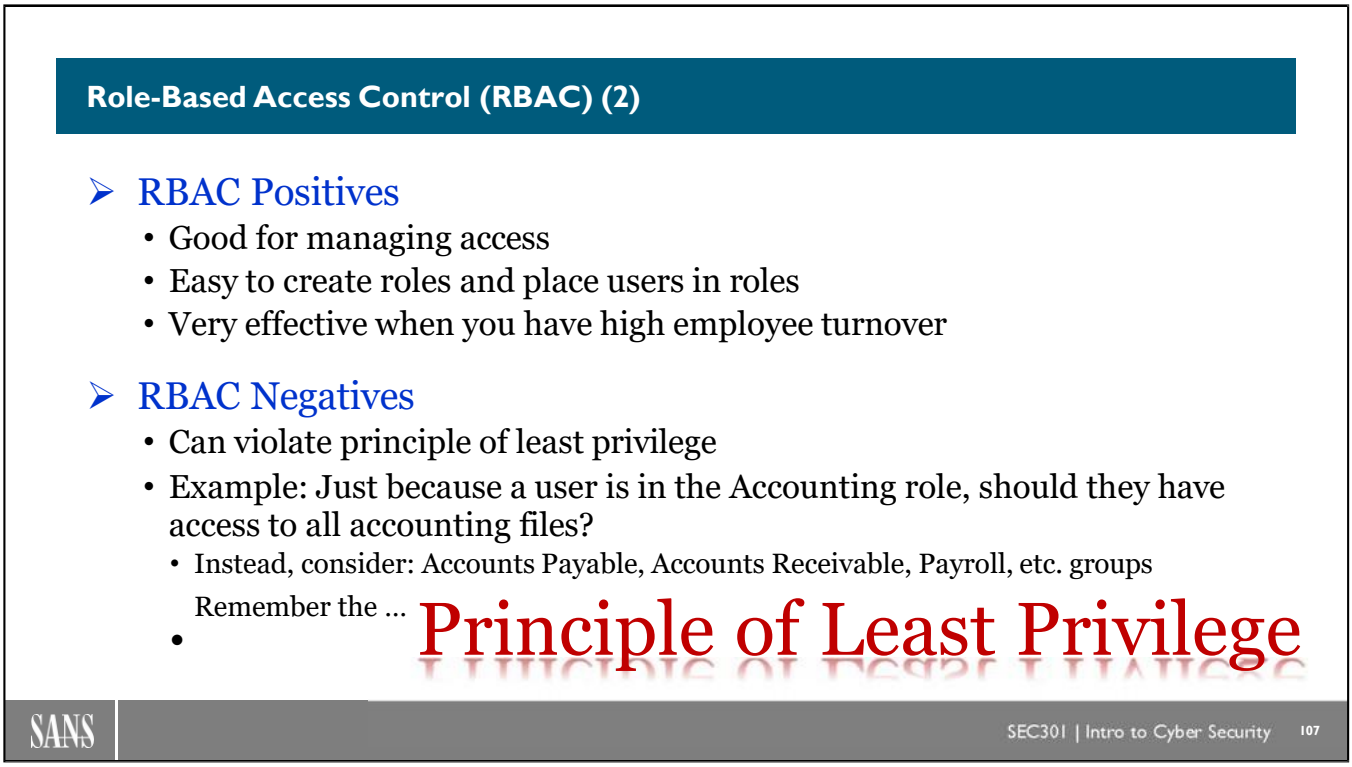
Role-Based Access Controls are the most common method used today for controlling access to various resources. They are also possible in Windows, UNIX, and Linux; you just have to set it up and configure it.

Here, the administrator creates a "group plan." In other words, what groups will be necessary and what accesses should each group have. Then, as a new user comes into the organization, the administrator creates a user account and assigns the account to the appropriate group or groups based on the user's role within the company (or what tasks the user will need to perform in their job).

For example, when Joe comes to work for the company and is going to work in accounting, we might create an account named *Joe* and place that account into the *Accounting* group. That group affiliation gives Joe access to everything in the Accounting department, so he can do his work. (We will continue this example on the following page.)

The real secret to success here is the group plan: Creating the appropriate groups and *only* assigning the required permissions to each. Remember, this is a primary method of implementing the Principle of Least Privilege: Everyone can do everything they need to do, *and nothing more*.

Note: Role-Based Access Control (RBAC) will also sometimes be called Task-Based Access Control or TBAC.



Role-Based Access Control (RBAC) 2

Like most things in security, RBAC is about trade-offs. In other words, it has its good points and its bad points.

On the positive side, they are easy to manage when compared to other access control models. With some thought, it is not too difficult to determine the correct roles, create the groups representing those roles, and assign the proper permissions. RBAC especially lends itself to managing access in an organization with high employee turnover. Each user only requires a basic account with access to their own files. That account is then assigned to appropriate pre-existing groups, granting them the access needed to do their jobs.

The drawbacks of RBAC are pretty serious, though. Unless you implement them correctly, they lead to massive breaches, ransomware gone wild, etc. Too many companies implement RBAC by creating a single group called *users*. Everyone in the company belongs to the user's group and any member of the user's group can access anything in the company. Think what this means if a phishing email leads to the compromise of a users credentials. The attackers can now access that user's account and that account can access everything in the company.

Let's return to our example from the previous page. Joe came to work for the company in the Accounting Department. We created an account named *Joe* and put that account into the Accounting group. That group affiliation gives the user Joe access to everything in the Accounting Department. But Joe is going to work in Accounts Receivable and does not require access to everything else in Accounting, such as Accounts Payable, Payroll, etc. This is a failure of the **Principle of Least Privilege**.

Logging and Auditing
Privilege Audits

Accountability

Accountability

We are now ready to talk about accountability issues. In this section, we will look at:

- Logging and Auditing
- Privilege Audits

Logging and Auditing

Logs are essential for maintaining computer systems and the networks they create. There are many times that, without proper logs, the system and network administrators simply would not be able to troubleshoot problems.

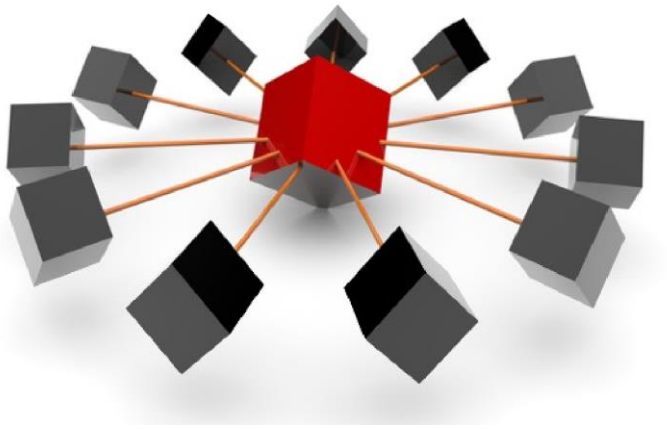
Logs are also critical to the security function. So far, we have gone to the trouble of verifying identity through authentication. We have implemented controls of which subject can access which object. Now we turn to the logs to find out what happened. Were there authentication failures? Was someone able to access a file they were not supposed to be able to access?

We know you have heard it before—everyone in IT has. But far too many of us ignore the advice anyway. *Logs MUST be reviewed on a regular basis*. The importance of this cannot be overstated. Most of the time when you are looking at logs (either for administration or security) you are looking for abnormal. If you do not review your logs regularly, then you have no idea what normal is. Until you can define normal, it is literally impossible to define abnormal. So, if you do not review your logs regularly, you cannot possibly locate problems.

Regular reviews lead you to discover trend information that creates your baselines. With baselines, you can then start using clipping levels to generate alerts or alarms when something out of the ordinary occurs. For example, it is normal to see the occasional bad login attempt to the administrator account. Seeing 40 bad login attempts in under a minute indicates an online brute-force tool is being used. In this case, 40 attempts in under a minute is the threshold that becomes your clipping level.

An Unbreakable Rule: Admins cannot have access to their final logs!

Logs in Court



- Can logs be used in court?
  - Maybe… It depends on many factors.
- Can we make it more likely?
  - YES!
- Use centralized log servers:
  - Admins have no access to central logs
  - Digitally sign log files immediately after a log switch
  - Compare local logs to central logs to find deleted entries

Logs in Court

A common question that arises is, “Can computer generated logs be used in court?” The answer to this question is, “Maybe, but it depends on many factors.” Which judge will preside over the case? Is it a local, state, or federal court? What country is the court in and what country were the logs generated in? We could easily fill many pages with just the questions without ever getting to the answers.

Perhaps the better approach is to answer this question instead: “Can we do something to make it more likely that our computer generated logs will be admitted and believed in court?” To that question we can give a definitive yes.

Generally, before a court will accept and believe computer-generated evidence, you need to be in a position to "prove the veracity of the evidence.” In other words, prove that the logs were not typed up by a human (or otherwise edited), and that they are a true and complete record of what happened. To say it more simply, you have to prove the logs have not been edited by a human in any way.

Logs are typically edited for one of two reasons.

- First, a hacker is trying to hide their tracks.
- Second, a system administrator did something unauthorized and does not want you to know about it.

Perhaps the best way to help prove logs remain pristine is to utilize central log servers and never break an unbreakable rule which says:

System Administrators cannot have final access to their logs!

Here is what that means.

- When a computer generates a log entry, two things happen simultaneously
    - A copy of the log entry is written to a local file
    - A copy of the log entry is sent to a central log server
- The administrator of the system generating the log entry
    - Uses the local log entry to administer their system
    - Has NO ACCESS to the central log server
- Once the log file is full, the central log server automatically
    - Switches the filled log file to a new file and starts creating a fresh log file
    - The filled file is immediately digitally signed
    - The digitally signed log file is shipped to a central storage repository
    - Note – this entire process is automatic and requires no human interaction

By putting this in place, it becomes much easier to show a court that the log files have not been tampered with. Maintaining this system also has a second advantage.

Let's say the log file on the administrator's local computer HAS been modified. If you simply take the modified file and the digitally signed file and compare them, it becomes immediately obvious what someone does not want you to see. Anything missing from the local computers file is what someone has deleted.

SEC301.1 | Introduction to Cyber Security

SANS

Security's Foundation

End Day 1

This page intentionally left blank.

This page intentionally left blank.

SANS

Module Review Questions

This page intentionally left blank.

SANS

Core Principles Review Question

This page intentionally left blank.

- The elements of the CIA follow (choose 3):
  A. Authentication
  B. Integrity
  C. Authorization
  D. Confidentiality
  E. Availability
  F. Cryptography
  G. Impersonation

This page intentionally left blank.

- Which role always has ultimate responsibility for security in an organization?
  A. Custodian
  B. User
  C. Senior Manager
  D. Owner

- What is the goal of most cyber threats today?
  A. Ransom
  B. Make money for the attacker
  C. Obtain online banking credentials
  D. Obtain credit cards

This page intentionally left blank.

- What is the name of the role with primary responsibility for data?
  A. Senior Manager
  B. Data Owner
  C. Data Custodian
  D. Data User

- Which role is responsible for implementing controls on data?
  A. Data Custodian
  B. Senior Manager
  C. Security Manager
  D. Data Owner

This page intentionally left blank.

SANS

Risk Management Review Questions

This page intentionally left blank.

Risk Management

Review Questions (1)

- The term Due Care means senior management has a legal responsibility to:
  A. Act as a reasonable person would act in protecting assets
  B. Follow industry best practices in the security program
  C. Prevent your organization from being a tool to hurt another
  D. Due care is not actually a legal requirement

- Who in the organization determines if risk is acceptable?
  A. Chief Executive Officer (CEO)
  B. Data Owner
  C. Chief Information Officer (CIO)
  D. Chief Security Officer (CSO)

This page intentionally left blank.

- The term Exposure Factor means:
  A. What it costs each time a threat materializes
  B. The annual frequency that a threat occurs
  C. The likelihood that a threat will occur
  D. The percentage of asset value loss

- The term Single Loss Expectancy means:
  A. What it costs each time a threat materializes
  B. The annual frequency that a threat occurs
  C. The likelihood that a threat will occur
  D. The percentage of asset value loss

This page intentionally left blank.

Risk Management

Review Questions (3)

- The formula to arrive at Annual Loss Expectancy is:
  A. Exposure Factor * Single Loss Expectancy
  B. Annual Rate of Occurrence * Single Loss Expectancy
  C. Annual Rate of Occurrence * Exposure Factor
  D. Asset Value * Exposure Factor

- The formula to arrive at Single Loss Expectancy is:
  A. Exposure Factor * Single Loss Expectancy
  B. Annual Rate of Occurrence * Single Loss Expectancy
  C. Annual Rate of Occurrence * Exposure Factor
  D. Asset Value * Exposure Factor

This page intentionally left blank.

- There are two approaches to Risk Assessment: Quantitative and Qualitative

- Which is based on money?
  A. Qualitative
  B. Quantitative

- Which is based on severity and likelihood?
  A. Qualitative
  B. Quantitative

This page intentionally left blank.

- Of the three control areas, which deals with user account login authentication?
  A. Administrative Controls
  B. Confidentiality Controls
  C. Technical Controls
  D. Physical Controls

- Of the three control types, which deals with authentication?
  A. Preventive
  B. Detective
  C. Responsive
  D. Corrective

This page intentionally left blank.

- Which Risk Strategy deals with stopping risky activities or business practices?
  A. Risk Mitigation
  B. Risk Avoidance
  C. Risk Deterrence
  D. Risk Transference

- Which Risk Strategy involves buying insurance?
  A. Risk Mitigation
  B. Risk Avoidance
  C. Risk Deterrence
  D. Risk Transference

This page intentionally left blank.

SANS

Policy Review Question

This page intentionally left blank.

- Separation of duties means:
  A. No person has control of a critical process from beginning to end
  B. No person can access data alone; it takes two people
  C. Personnel are rotated through critical positions
  D. Two managers must sign off on all decisions

- If completed correctly, a Non-Disclosure Agreement (NDA) is a legally binding contract:
  A. True
  B. False

This page intentionally left blank.

Security Policy

Review Questions (2)

- What defines and dictates effective policy in any organization?
  A. The corporate culture of the organization
  B. Legal requirements always dictate policy
  C. The desires of senior management
  D. The whims of the Chief Security Officer

- All awareness training must be:
  A. Documented
  B. Conducted face-to-face
  C. Conducted by senior management
  D. Performed once and never again

This page intentionally left blank.

- A broad, general statement of management intent defines:
  A. A procedure
  B. A waste of time
  C. A policy

- Dual control means:
  A. No person has control of a critical process from beginning to end
  B. No person can access data alone; it takes two people
  C. Personnel are rotated through critical positions
  D. Two managers must sign off on all decisions

This page intentionally left blank.

SANS

AAA Review Question

This page intentionally left blank.

Review Questions (1)

- Authentication is:
  A. The process of verifying identity
  B. The process of entering a password
  C. A process that allows one computer to talk to another
  D. Not effective in today's environment

- Three common authentication factors are (choose 3):
  A. Something you know
  B. Something you would like to be
  C. Somewhere you are
  D. Something you have
  E. Something you are

This page intentionally left blank.

Review Questions (2)

- Maximum password aging is:
  A. When you are not allowed to change a password for a period of time
  B. When you must change your password after a period of time
  C. Not possible on most computers
  D. When you cannot reuse a password for a period of time

- Minimum password aging must always be shorter than maximum password aging:
  A. True
  B. False

This page intentionally left blank.

Review Questions (3)

- John the Ripper is an example of:
  A. Password history software
  B. A password generator
  C. Password management software
  D. Password cracking software

- Cognitive passwords:
  A. Must always be factual
  B. Ask a question only you know the answer to
  C. Ask you to type in a series of letters from a graphic
  D. Ask you to answer a question that you answered previously

This page intentionally left blank.

Review Questions (4)

- "Something you have" authentication is also:
  A. Biometrics (that is, you have a fingerprint)
  B. A token you hold in your hand
  C. Based on the fact that you possess the computer you are logging into
  D. Always require the use of a PIN number

- One-time passwords strive to defeat which attack?
  A. Mathematical attack
  B. Password guessing attack
  C. Dictionary attack
  D. Replay attack

This page intentionally left blank.

Review Questions (5)

- An authentication system that requires you to authenticate using a username, password, and PIN number is:
  A. A two-factor authentication system
  B. A multi-factor authentication system
  C. A something-you-have authentication system
  D. A single-factor authentication system

- Another term for two-factor authentication is:
  A. 2FA
  B. Strengthened authentication
  C. 3FA
  D. Overkill

This page intentionally left blank.

Review Questions (6)

- Which access control model relies on job function?
  A. Role-Based Access Control (RBAC)
  B. Discretionary Access Control (DAC)
  C. Functional Access Control (FAC)
  D. Rule-Set Base Access Control (RSBAC)

- What is the most common form of access control used today?
  A. Functional Access Control (FAC)
  B. Role-Based Access Control (RBAC)
  C. The Principle of Least Privilege
  D. Mandatory Access Control (MAC)

This page intentionally left blank.

Review Questions (7)

- In court, computer-generated evidence is considered what type of evidence until a judge rules otherwise?
  A. Best evidence
  B. Hearsay evidence
  C. Corroborative evidence
  D. Supportive evidence

This page intentionally left blank.

SANS

Answers to Review Questions

This page intentionally left blank.

SANS

Core Principles Review Question Answers

This page intentionally left blank.

- The elements of the CIA are:
  A. Authentication
  B. Integrity
  C. Authorization
  D. Confidentiality
  E. Availability
  F. Cryptography
  G. Impersonation

This page intentionally left blank.

- Which role always has ultimate responsibility for security in an organization?
  A. Custodian
  B. User
  C. Senior Manager
  D. Owner

- What is the goal of most Cyber Threats today?
  A. Ransom
  B. Make money for the attacker
  C. Obtain online banking credentials
  D. Obtain credit cards

This page intentionally left blank.

- What is the name of the role with primary responsibility for data?
  A. Senior manager
  B. Data Owner
  C. Data Custodian
  D. Data User

- What role is responsible for implementing controls on data?
  A. Data Custodian
  B. Senior manager
  C. Security manager
  D. Data Owner

This page intentionally left blank.

SANS

Risk Management Review Question Answers

This page intentionally left blank.

- The term *due care* means that senior management has a legal responsibility to:
  - **A. Act as a reasonable person would act in protecting assets**
  - B. Follow industry best practices in the security program
  - C. Prevent your organization from being a tool to hurt another
  - D. Due care is not actually a legal requirement

- Who in the organization determines if risk is acceptable?
  - **A. Chief Executive Officer (CEO)**
  - B. Data Owner
  - C. Chief Information Officer (CIO)
  - D. Chief Security Officer (CSO)

This page intentionally left blank.

- The term Exposure Factor means:
  A. What it costs each time a threat materializes
  B. The annual frequency that a threat occurs
  C. The likelihood that a threat will occur
  D. <u>The percentage of asset value loss</u>

- The term Single Loss Expectancy means:
  A. <u>What it costs each time a threat materializes</u>
  B. The annual frequency that a threat occurs
  C. The likelihood that a threat will occur
  D. The percentage of asset value loss

This page intentionally left blank.

- The formula to arrive at Annual Loss Expectancy is:
  A. Exposure Factor * Single Loss Expectancy
  B. Annual Rate of Occurrence * Single Loss Expectancy
  C. Annual Rate of Occurrence * Exposure Factor
  D. Asset Value * Exposure Factor

- The formula to arrive at Single Loss Expectancy is:
  A. Exposure Factor * Single Loss Expectancy
  B. Annual Rate of Occurrence * Single Loss Expectancy
  C. Annual Rate of Occurrence * Exposure Factor
  D. Asset Value * Exposure Factor

This page intentionally left blank.

- There are two approaches to Risk Assessment: Quantitative and Qualitative

- Which is based on money?
  A. Qualitative
  B. <u>Quantitative</u>

- Which is based on severity and likelihood?
  A. <u>Qualitative</u>
  B. Quantitative

This page intentionally left blank.

- Of the three control areas, which deals with your user account login authentication?
  - A. Administrative Controls
  - B. Confidentiality Controls
  - **C. Technical Controls**
  - D. Physical Controls

- Of the three control types, which deals with authentication?
  - **A. Preventive**
  - B. Detective
  - C. Responsive
  - D. Corrective

This page intentionally left blank.

- Which Risk Strategy deals with stopping risky activities or business practices?
  - A. Risk Mitigation
  - **B. Risk Avoidance**
  - C. Risk Deterrence
  - D. Risk Transference

- Which Risk Strategy involves buying insurance?
  - A. Risk Mitigation
  - B. Risk Avoidance
  - C. Risk Deterrence
  - **D. Risk Transference**

This page intentionally left blank.

SANS

Policy Review Question Answers

This page intentionally left blank.

- Separation of duties means:
  A. No person has control of a critical process from beginning to end
  B. No person can access data alone; it takes two people
  C. Personnel are rotated through critical positions
  D. Two managers must sign off on all decisions

- If completed correctly, a Non-Disclosure Agreement (NDA) is a legally binding contract:
  A. True
  B. False

This page intentionally left blank.

Policy

Review Questions (2)

- What defines and dictates proper policy in any organization?
  - **A. <u>The corporate culture of the organization</u>**
  - B. Legal requirements always dictate policy
  - C. The desires of senior management
  - D. The whims of the Chief Security Officer

- All awareness training must be:
  - **A. <u>Documented</u>**
  - B. Conducted face-to-face
  - C. Conducted by senior management
  - D. Performed once and never again

This page intentionally left blank.

Review Questions (3)

- A broad, general statement of management intent defines:
  A. A procedure
  B. A waste of time
  C. A policy

- Dual control means:
  A. No person has control of a critical process from beginning to end
  B. No person can access data alone; it takes two people
  C. Personnel are rotated through critical positions
  D. Two managers must sign off on all decisions

This page intentionally left blank.

SANS

AAA
Review Question Answers

This page intentionally left blank.

Review Questions (1)

- Authentication is:
  - **A. The process of verifying identity**
  - B. The process of entering a password
  - C. A process that allows one computer to talk to another
  - D. Not effective in today's environment

- Three common authentication factors are:
  - **A. Something you know**
  - B. Something you would like to be
  - C. Somewhere you are
  - **D. Something you have**
  - **E. Something you are**

This page intentionally left blank.

Review Questions (2)

- Maximum password aging is:
  A. When you are not allowed to change a password for a period of time
  B. When you must change your password after a period of time
  C. Not possible on most computers
  D. When you cannot reuse a password for a period of time

- Minimum password aging must always be shorter than maximum password aging:
  A. True
  B. False

This page intentionally left blank.

Review Questions (3)

- John the Ripper is an example of:
  A. Password history software
  B. A password generator
  C. Password management software
  D. Password cracking software

- Cognitive passwords:
  A. Must always be factual
  B. Ask a question only you know the answer to
  C. Ask you to type in a series of letters from a graphic
  D. Ask you to answer a question that you answered previously

This page intentionally left blank.

Review Questions (4)

- "Something you have" authentication is also:
  A. Biometrics (that is, you have a fingerprint)
  B. A token you hold in your hand
  C. Based on the fact that you possess the computer you are logging into
  D. Always require the use of a PIN number

- One-time-passwords strive to defeat which attack?
  A. Mathematical attack
  B. Password guessing attack
  C. Dictionary attack
  D. Replay attack

This page intentionally left blank.

Review Questions (5)

- An authentication system that requires you to authenticate using a username, password, and PIN number is:
  A. A two-factor authentication system
  B. A multi-factor authentication system
  C. A something-you-have authentication system
  D. A single-factor authentication system

- Another term for two-factor authentication is:
  A. 2FA
  B. Strengthened authentication
  C. 3FA
  D. Overkill

This page intentionally left blank.

Review Questions (6)

- Which access control model relies on job function?
  - **A. Role-Based Access Control (RBAC)**
  - B. Discretionary Access Control (DAC)
  - C. Functional Access Control (FAC)
  - D. Rule-Set Base Access Control (RSBAC)

- What is the most common form of access control used today?
  - A. Functional Access Control (FAC)
  - **B. Role-Based Access Control (RBAC)**
  - C. The Principle of Least Privilege
  - D. Mandatory Access Control (MAC)

This page intentionally left blank.

Review Questions (7)

- In court, computer-generated evidence is considered what type of evidence until a judge rules otherwise?
  A. Best evidence
  B. Hearsay evidence
  C. Corroborative evidence
  D. Supportive evidence

This page intentionally left blank.

Many of the slide graphics in this course are provided through a royalty-free license with PresentationPro. http://www.presentationpro.com/