JOHNS HOPKINS
CAREY BUSINESS SCHOOL

Introduction to Cybersecurity

Module #1

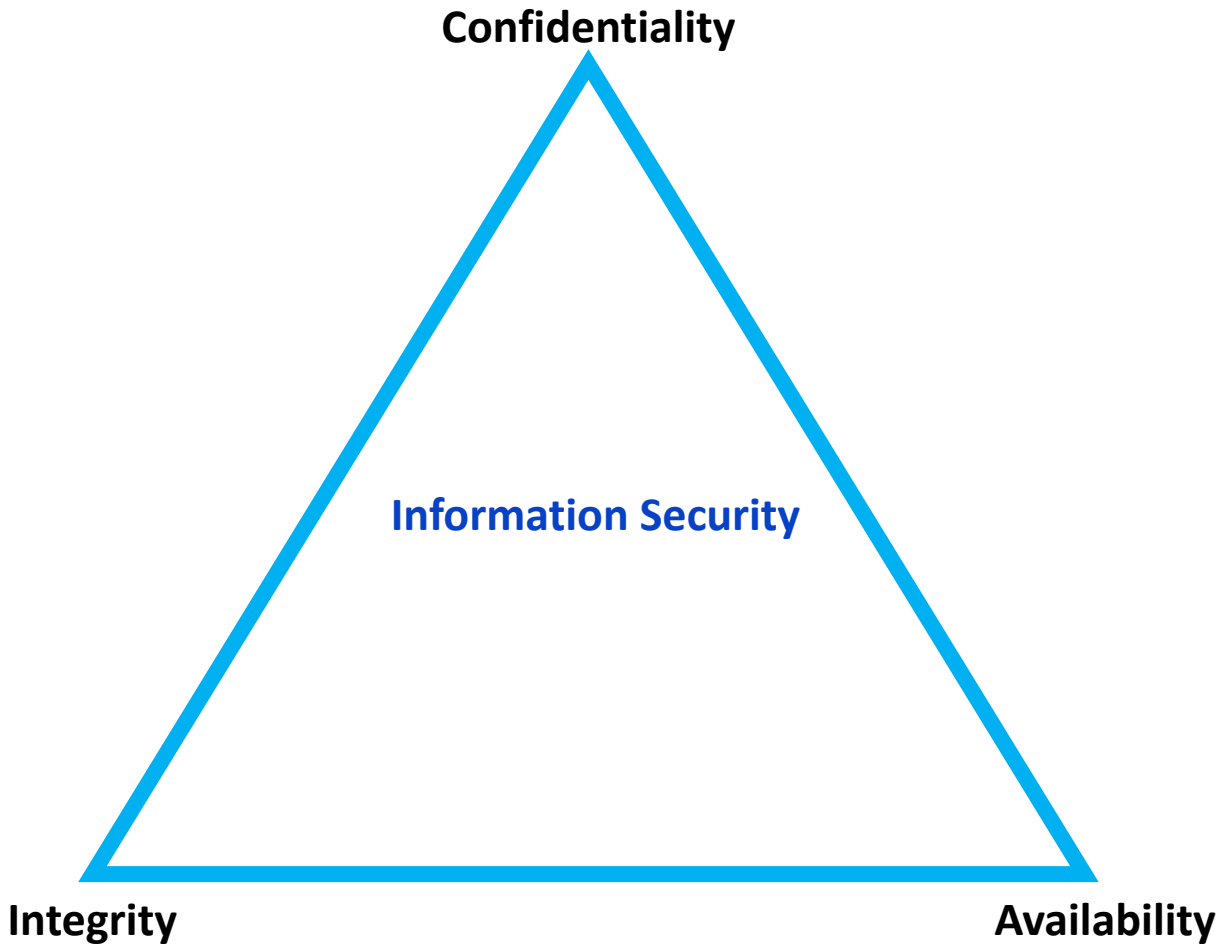
Introductions, Expectations and Course Objectives • Why is Cybersecurity Important? • Guiding Principles and Paradigms in Cybersecurity • The C-I-A Triangle • The US ODNI-recommended Cyber Threat Framework (CTF) • Telecomm Made Simple: The Five Main Components • The Beginnings of Our Cybersecurity Lexicon • Previews of Your Group Project: Creating a Cybersecurity Assessment for an Organization in Turmoil

Module #1

The C-I-A Triangle

The C-I-A Triad

The Cornerstones of Cybersecurity



The C-I-A Triad

Confidentiality

Limiting access to information to only those who need it, and preventing access by those who don't

- Confidentiality protection measures:
  - Information classification
  - Secure document (and data) storage
  - Application of general security policies
  - Education of information custodians and users
  - Cryptography (encryption)

The C-I-A Triad

Availability

Users, either people or systems, have access to information in a usable format

- Examples of events that could impact availability include:
  - Natural disaster
  - Distributed Denial of Service (DDoS)
  - Hardware and/or software failure
- Availability safeguard measures:
  - Data backup
  - Business continuity planning

The C-I-A Triad

Integrity

Completeness of information is threatened when exposed to corruption, damage, destruction or alteration of its authentic state

- Loss of integrity is almost worse than loss of data:
  - How do you know what has been changed?
  - What decisions are made based upon inaccurate data?

Module #1

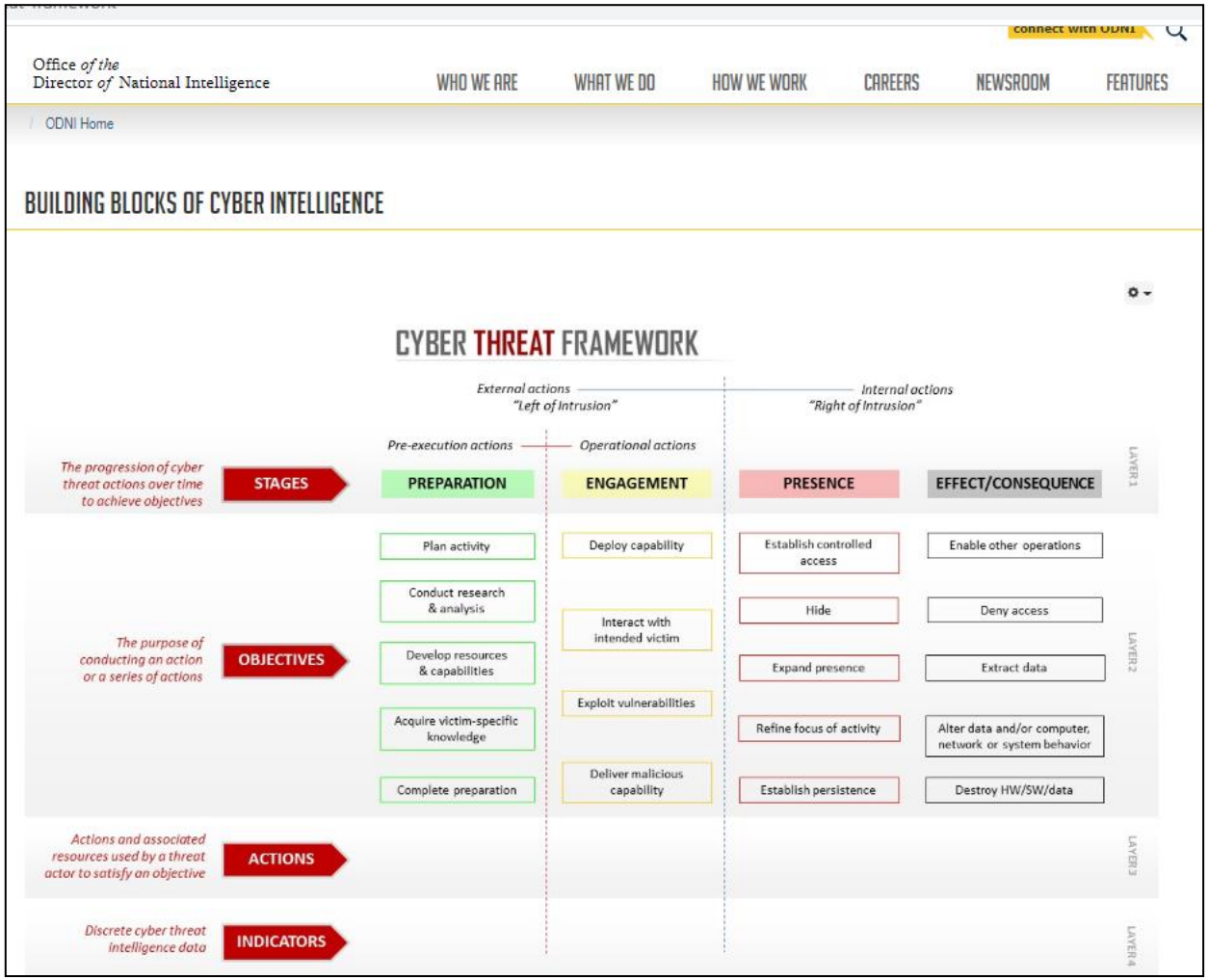
The US ODNI-recommended Cyber Threat Framework (CTF)

Preferred Model(s): The Cyber Threat Framework (CTF)

How should one think about observed malicious network activity?

The United States' Office of the Director of National Intelligence- or ODNI-endorsed Cyber Threat Framework (CTF) was created to allow ease in communication between stakeholders of information network security. It does this by:
(1) simplifying the categorization of observed online malicious activities and behaviors; and (2) creating a lexicon which must be used by cyber threat analysts in the US intelligence community to describe these activities and behaviors.

More information and details on the CTF may be found here: https://www.dni.gov/index.php/cyber-threat-framework



Preferred Model(s): The Cyber Threat Framework (CTF)

How are the Four Stages of the CTF Defined/Characterized?

LAYER 1 - STAGES				
PREPARATION	ENGAGEMENT	PRESENCE		EFFECT
Actions to prepare to conduct cyber activities	*Actions to gain unauthorized access*	*Actions to maintain unauthorized access*		*Outcomes of actions on targeted system*
LAYER 2 - STAGES				
Plan Activity	Deploy Capability	Establish Initial Control	Establish Persistence	Deny access
Research & Analysis	Interact with Target	Hide	Expand Presence	Alter System Behavior
Resource/Capability Development	Drive-by attacks	Refine Targeting		Extract data
Conduct Reconnaissance	Exploit Vulnerabilities			Destroy HW/SW/Data
Stage Capabilities	Deliver Payload			Enable Other Operations
Initiate Operations	Suspicious Network Activity			
LAYER 3 - STAGES				
Review Strategy	Deploy Electronically	Unauthorized access	Anti-intrusion Detection Measures	Disrupt/Degrade Links
Plan Mission	Physical Proximity	Automated Malware C2	Anti-forensic measures	Disrupt/Degrade Network
Issue Guidance	Credential Farming	Establish Communications	Monitor Administrators	DDoS
Gather Intelligence	Social Engineering	Network Mapping	Increase User Privileges	Install Ransomware
Identify Targets	SQL Injection	Software Packing	Lateral Movement	Create Botnet(s)
Develop Infrastructure	Masquerade	Masquerading	Identify Targets of Opportunity	Deface Websites
Physical Reconnaissance	Use of Exploit Kit	Obfuscate Payloads	Service Manipulation	Relocate/Store Data
Electronic Reconnaissance	Cross Site Scripting	Indicator Blocking	Registry Run Keys	Disclose Data
Stage Externally/Internally	Webmail Vulnerability	Scripting	BIOS Rootkit	Exfiltrate Data
Issue Operational Tasking	App Vulnerability	Disabling Security Tools	Master Boot Record	Establish C2 or Hop Point

Module #1

Telecomm Made Simple:

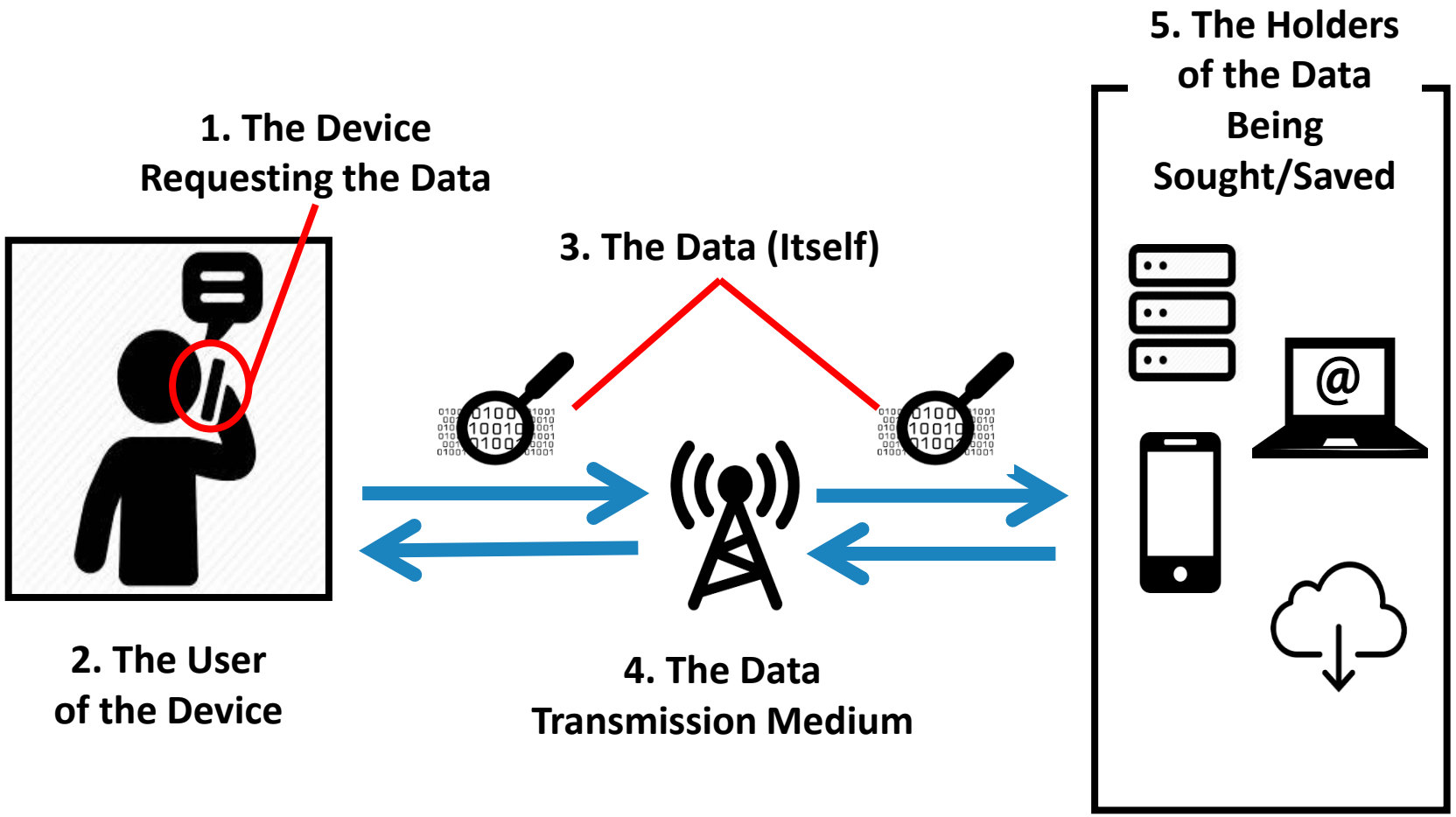
The Five Main Components

Telecomm Made Simple: The Five Main Components

What is it that We Need to Protect or Reinforce via Cybersecurity? (Avenues of Ingress and Egress)

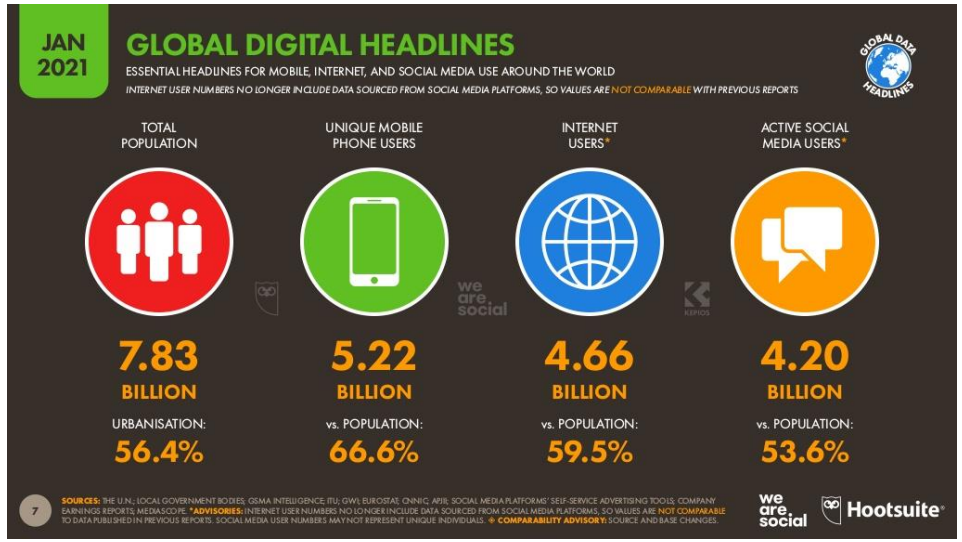
The Five Main Components

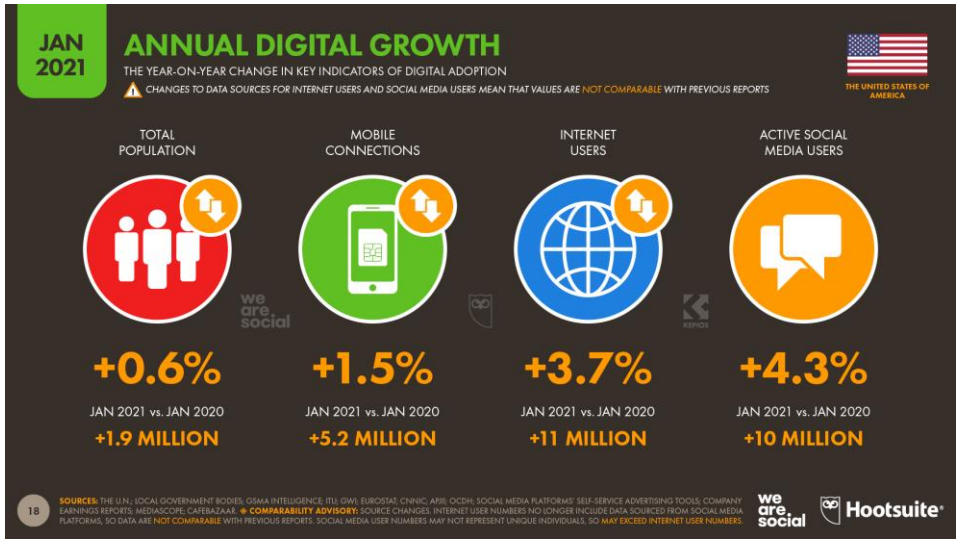
1. The Device Requesting the Data; frequently known as *the client*.
2. The User of the Device
3. The Data (Itself)
4. The Data Transmission Medium
5. The Holders of the Data Being Sought/Saved; frequently known as either *a host or server*. (*Note: The difference between the two will be discussed in later classes.)



Telecomm Made Simple: The Five Main Components

The User of the Device: Hello! Can you help me with an information request or service, please?



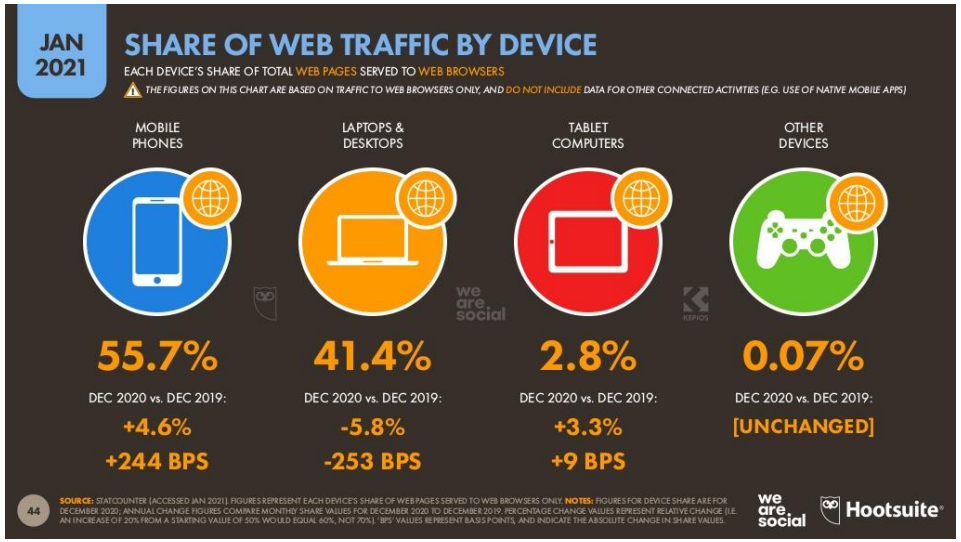


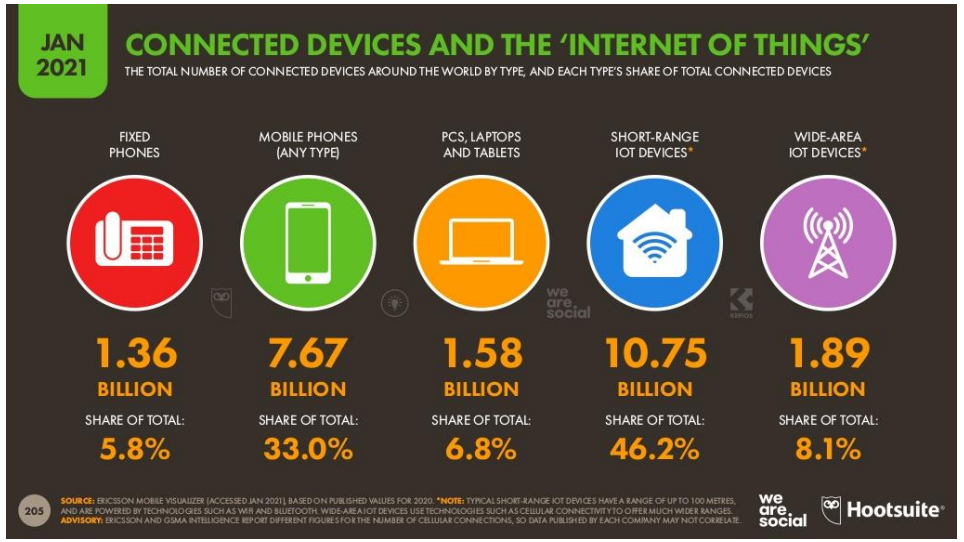
- There are a tremendous number of internet users around the world! Unfortunately, users of digital devices - and related accesses - are notoriously **THE BIGGEST THREATS** to information security due to lax or complete non-compliance with communications and information security protocols. Further, being the victim of social engineering and phishing scams are among the most prevalent pitfalls facing users of information networks who are continually the targets of malicious cyber actors.

***To view more outstanding visuals and great information – such as that in the graphics above - on the behaviors of "digital denizens" from around the world broken down by country, the originating document may be found in Course Documents. The source URL for the originating document is*: https://wearesocial.com/digital-2021

Telecomm Made Simple: The Five Main Components

The Device Requesting the Data (aka, Client): What in the Whole Wide World Can I Fetch for You Today?





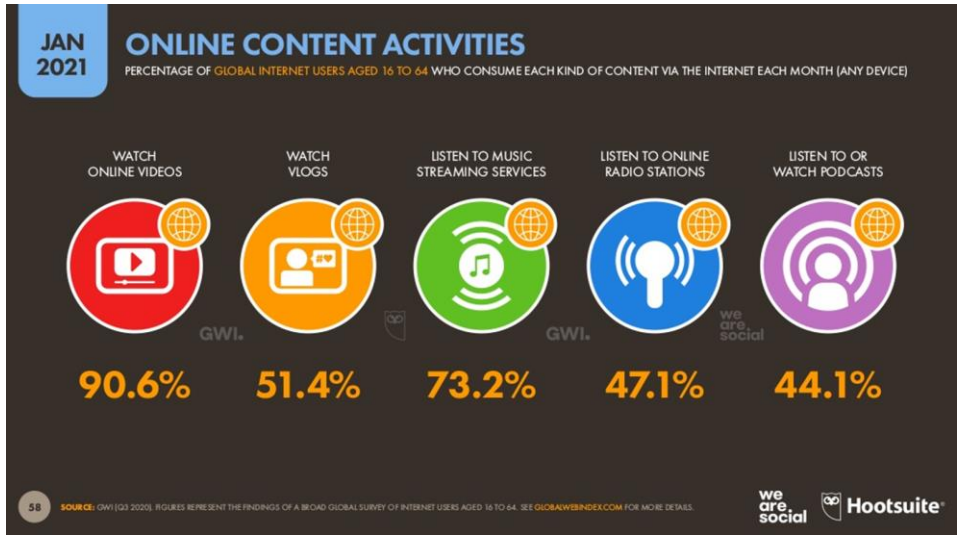
It should be remembered the device chosen to access online information will influence user behavior. The bad guys know this!!!

- As of February 2021, mobile had taken the lead at just below 55% of online usage, with desktop devices taking up about 42%. The remaining 2-3% can be attributed to tablets.
- When people make a purchase online, the "cart" gets bigger on a desktop. The average cart size was 24% higher from desktop users and 14% higher on tablets, respectively, than from mobile devices.
- The average number of seconds spent on a website in 2020 was 624 for mobile devices and 1,006 seconds for desktop machines.
- Smartphone usage makes up 80% of social media browsing; 95.1% on Facebook; 86% on Twitter; and 60% on LinkedIn.

Source: https://www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics

Telecomm Made Simple: The Five Main Components

The Data (Itself): What is the Nature of the Data We Seek or that We are Sending?



Data Formats: What Types of Data Formats are in Use?

- Think about the services and applications you enjoy using on a daily basis; These might include the following *(popular file extensions are in parentheses):
  - Writing a paper (.txt, .doc, .docx)
  - Checking/sending email (.msg, .emlx)
  - Creating/watching a video (.avi, .mpeg)
  - Using Spreadsheets (.xls, .xlxs, .csv)
  - Listening to music (.wav, .mp3)
  - Creating a static visual (.jpg, .tif, .png, .gif)
  - Creating a presentation (.pptx)

This list is by no means all-inclusive; There are innumerable online services sought by global network users and many file formats to support these services!

- During data transmission, all data – regardless of what kind of file or content they represent - are broken down into “1s” and “0s” known as binary. This is a basic “language” machinery can understand as all of the technologies supporting your services and requests “talk” to each other at blinding speeds!

Telecomm Made Simple: The Five Main Components

The Data Transmission Medium: Upon Which Roads does One's Data Travel?

Transmission: How does data get from "here" to "there"?

There two basic types of transmission media:

- Guided (tangible - i.e., wire or fiber) Ex.: Copper, Coax, Ethernet, Fiber optics
- Unguided (intangible - i.e., wireless) Ex.: WiFi, WiMax, SATCOM

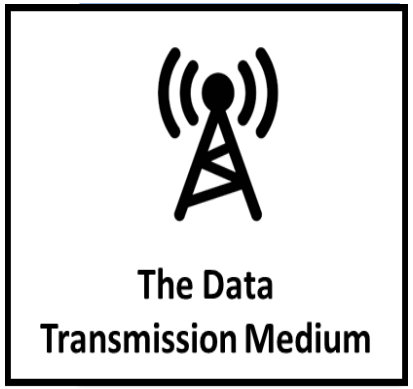
It is important to remember that regardless of how data is first ingested by a network at a point-of-presence (P-o-P) or access point, all data eventually rides over the very same communications infrastructure such as trunked fiber optic cables known commonly as "backbone". (see What does "trunked" mean?" in blue box). You may find a display and more info on backbone (submarine) cables at the following URL: https://www.ststworld.com/submarine-communications-cables/

Internet (Communication) Protocol(s): Are nothing more than **rules** that determine the format and transmission of data; implemented via hardware devices, software or both. The following are examples of highly used protocols:

- **Transmission Control Protocol (TCP)/Internet Protocol (IP)**
- **Hyper Text Transfer Protocol Secure (HTTPS)**
- **Post Office Protocols (POP)**
- **File Transfer Protocol (FTP)**

Think of protocols as the guides used to send data where you want them to go, and to bring the services you request back to you in a manner you can use.

How is this all done with optimal efficiency? Answer: MULTIPLEXING.



What does "trunked" mean?

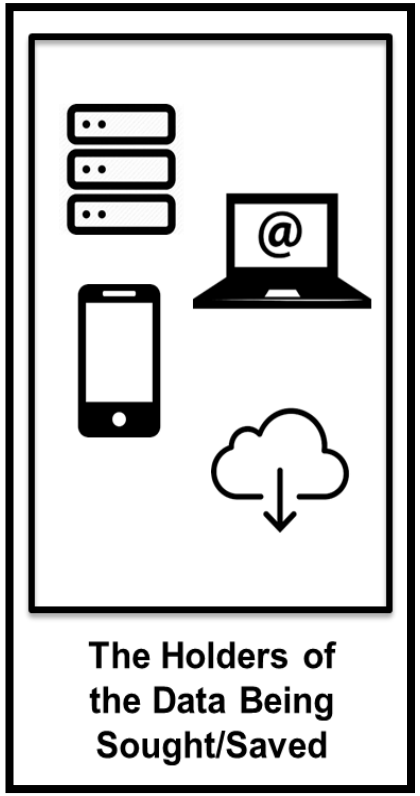
In a word: combined. Your information request gets combined with other requests from other users and sent – at light speed – along a number of fiber cables which have been "trunked" into one big cable lying at the bottom of the ocean. *Why is this important?* Your current and future use of **virtual private networks (VPNs)**! We will discuss VPNs especially when it involves the cybersecurity of larger, multinational enterprises!!!

Telecomm Made Simple: The Five Main Components

The Holders of Data Being Sought (e.g., Servers and Hosts): Hi! What do You Care to See AND are We Authorized to Provide it to You?

Information networks are useless to users if the information these users require cannot be accessed when they need it and in a format that is useable upon receipt. The devices and machines holding these data are programmed to ensure the user is who they say they are, the requested information is available, that access to the data is permitted, that any changes are recorded, and to ensure shifts in demand for the data are satisfied in a timely manner.

- A **database** is a collection of information that is organized so that it can be easily accessed, managed and updated. Computer databases typically contain aggregations of data records or files, containing information about sales transactions or interactions with specific customers.
- **Hosting** (also known as Web site hosting, Web hosting, and Webhosting) is the business of housing, serving, and maintaining files for one or more Web sites. More important than the computer space that is provided for Web site files is the fast connection to the Internet [which is NOT always present]. Most hosting services offer connections on T-carrier system lines.
- A **network server** is a computer system, which is used as the central repository of data (and databases) and various programs that are shared by users in a network.
- **Cloud computing** is internet technologies that provide software and storage as a service without needing the knowledge of how to create and operate the infrastructure that supports it.



What Is TCP Three-Way "HandShake"?

THREE-WAY HANDSHAKE or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client (requestor) and server (data holder) to exchange synchronization and acknowledgment packets before the real data communication process starts. Three-way handshake process is designed in such a way that both ends help a user to initiate, negotiate, and separate connections at the same time.

Module #1

The Beginnings of Our Cybersecurity Lexicon

The Beginnings of Our Cybersecurity Lexicon

Cybersecurity Key Terms

Attack – An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

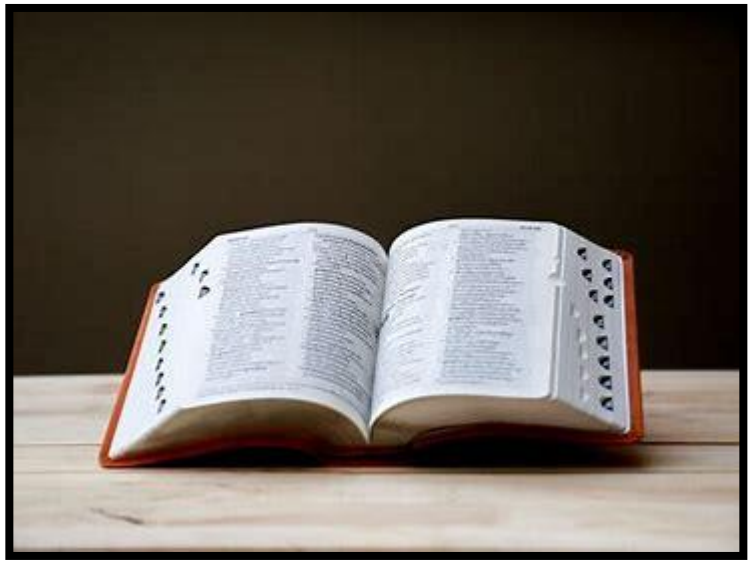
- *Extended Definition:* The intentional act of attempting to bypass one or more security services or controls of an information system.

Exploit – A technique to breach the security of a network or information system in violation of security policy.

Loss – The unauthorized and/or unexpected theft, damage, destruction or disclosure of an information asset *(*Six types of Loss in Cyber Incidents).*

Threat – A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

- *Extended Definition:* Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence.



The Most Common Sources of Cyber Threats

Who or What is the Threat Actor?

Threat agent: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. The most prevalent are:

- Nation states or national governments
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists and hackers
- Business competitors
- Disgruntled insiders

Vulnerability: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Threat Categories

What Events does Cybersecurity Help Practitioners Avoid or Mitigate?

Examples of Events:

- Insider threat (a.k.a., People) via incompetence, complicity, co-option, non-compliance, etc.
- Natural disaster *(e.g., force majeure)*
- Technological obsolescence and over-dependency
- Espionage
- Sabotage or vandalism
- Theft of Intellectual property or other enterprise assets
- Deviations in quality of service
- Unauthorized Access
- Information extortion
- Disruption to or destruction of hardware or software
- Hardware or software failures or errors

****Note: This list is by no means exhaustive, and represents those events which are believed to occur most frequently in connection with disruption or destruction of information systems.*

Today's Cybercrime Landscape

How do "They" Get What They Want? - Hacker Tactics, Techniques, and Procedures (TTPs)

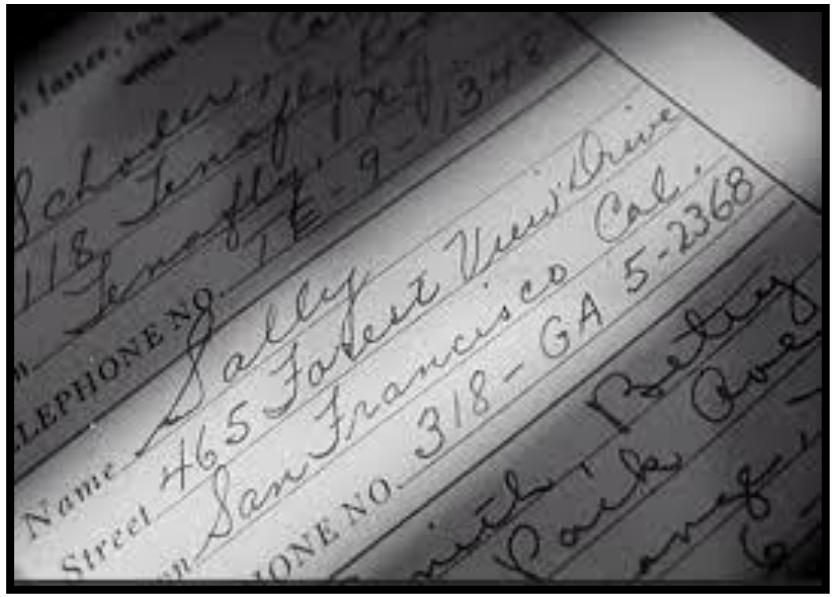
- Advanced Persistent Threats
- Ransomware
- Distributed Denial of Service (DDoS)
- Rogue Software
- Unpatched Software
- Wiper Attacks
- Intellectual Property Theft
- Botnets
- Data Destruction
- Spyware/Malware
- Man in the Middle (MITM)
- Drive-By Downloads
- Malvertising
- Data Manipulation
- Phishing
- Trojans
- Theft of Money

****Note: This list is by no means exhaustive, and represents those TTPs which are observed frequently in connection with disruption or destruction of information systems.*

What are (Most) Malicious Cyber Actors After? (1 of 2)

Personally Identifiable Information (PII) /Sensitive Personal Information (SPI)

- Full name
- Email address
- National ID #
- Passport #
- License plate #
- Drivers license #
- Fingerprints
- Credit card #
- Date of birth
- Birthplace
- Genetic information
- Telephone #
- Login name/screen name
- Group affiliations
- Familial Relations
- Purchasing activity
- IP Address/Log-in area



****Note: This list is by no means exhaustive, and represents a sample of that PII/SPI likely to be sought by malicious cyber actors.*

What are (Most) Malicious Cyber Actors After? (2 of 2)

Possible PII (depending on linkage)

- First or last name
- Country, state, post code, city of residence
- Age
- Gender or race
- Name of school they attend or workplace
- Grades, salary or job position
- Criminal record
- Web cookie
- Photographs (i.e., identifying logos, uniforms, etc.)

****Note: This list is by no means exhaustive, and represents a sample of that PII/SPI likely to be sought by malicious cyber actors.*

What can Information Assurance Practitioners Control?

The Six P's

- Plans
- Policymaking
- Protections
- Programs
- Personnel
- Project Management

Module #1

Previews of Your Group Project: Creating a Cybersecurity Assessment for an Organization in Turmoil

JOHNS HOPKINS
CAREY BUSINESS SCHOOL

Introduction to Cybersecurity

Module #2

Protection Mechanisms • Frameworks, Optics, and Models Used in Cybersecurity • Group Project: The Cybersecurity Assessment and Presentation • Affiliation/Situation: The Lone Entrepreneur and Sole Employed

Module #2

Protection Mechanisms

Protection Mechanisms

Introduction

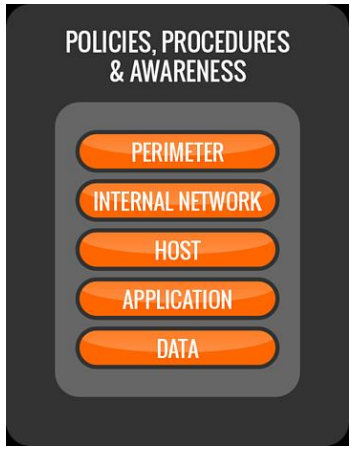
- **Technology alone cannot protect an organization's data and other assets!**
- Leveraging a Defense-in-Depth (DiD) is the best approach to securing any information network.
    - Foundations for DiD are based on use of people, policies AND technology.
- Technology controls can include (but are certainly NOT limited to) access controls, encryption, firewalls, anti-virus, software patches, etc.

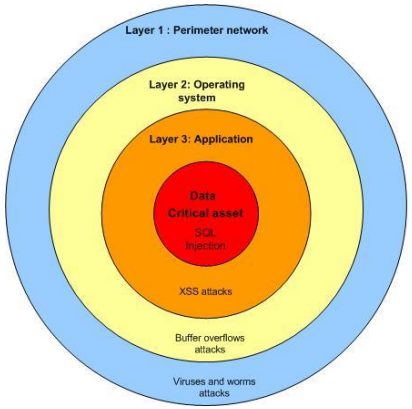
Protection Mechanisms

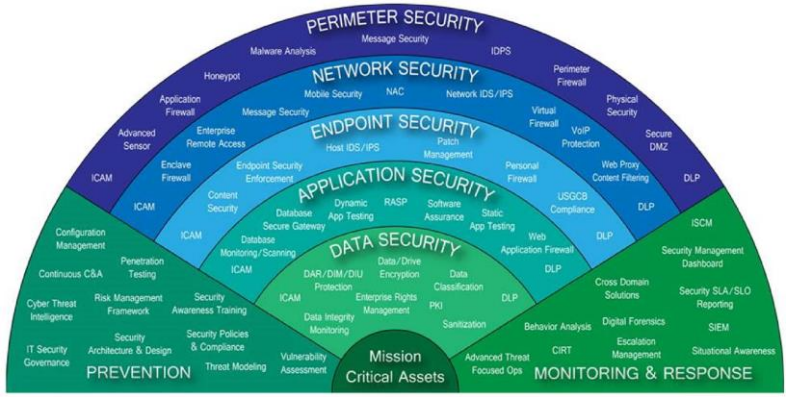
Defense-in-Depth (DiD)

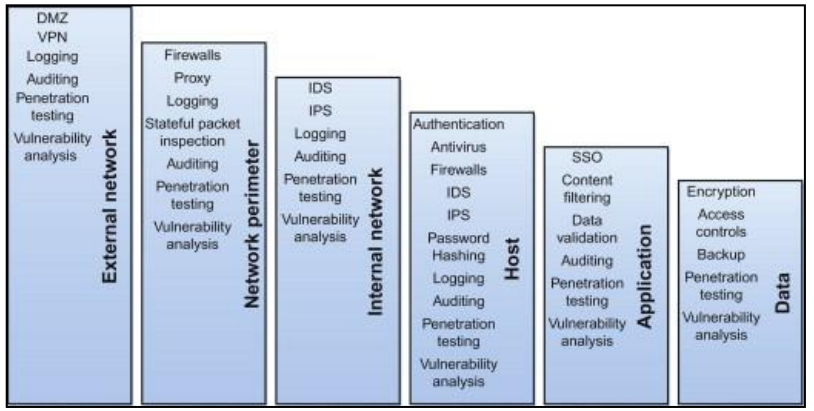
There are many models to be used, in innumerable conditions, to build a network's defense-in-depth. However, there four features for any DiD which are most important regardless of model chosen and conditions confronted:

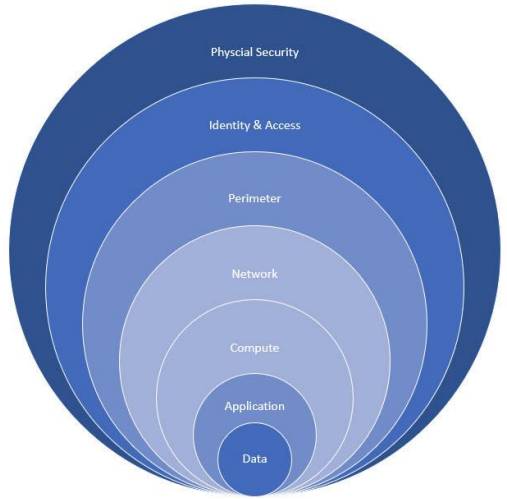
1. If possible, the defenses must be layered;
2. If possible, the status of the defenses must be measureable;
3. If possible, the defenses must operate independently of each other;
4. If possible, the defenses must be randomized (i.e., not operate cyclically) despite always being active.





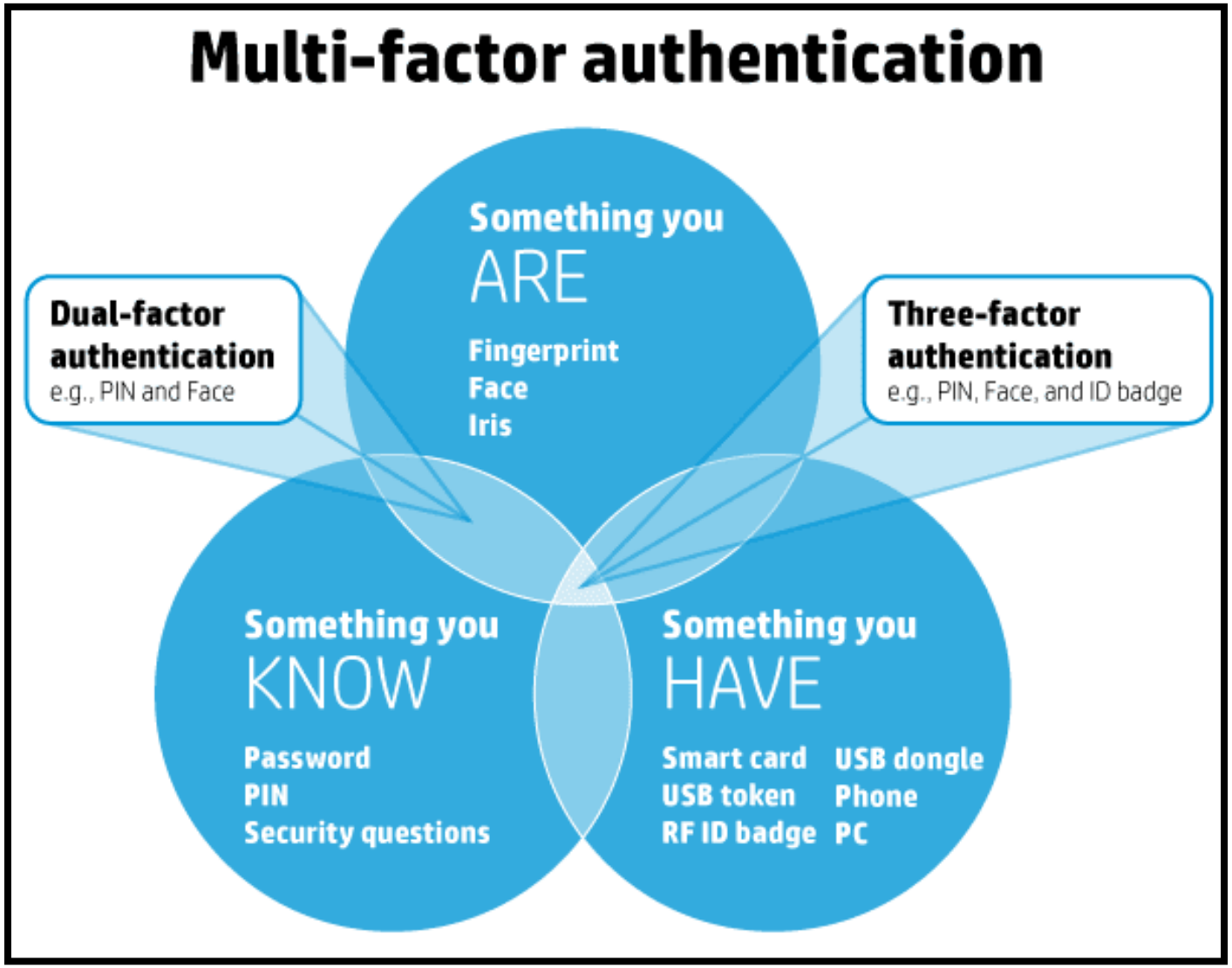






Protection Mechanisms

Access Controls and Biometrics – Multi-factor (2 or 3) Authentication



Protection Mechanisms

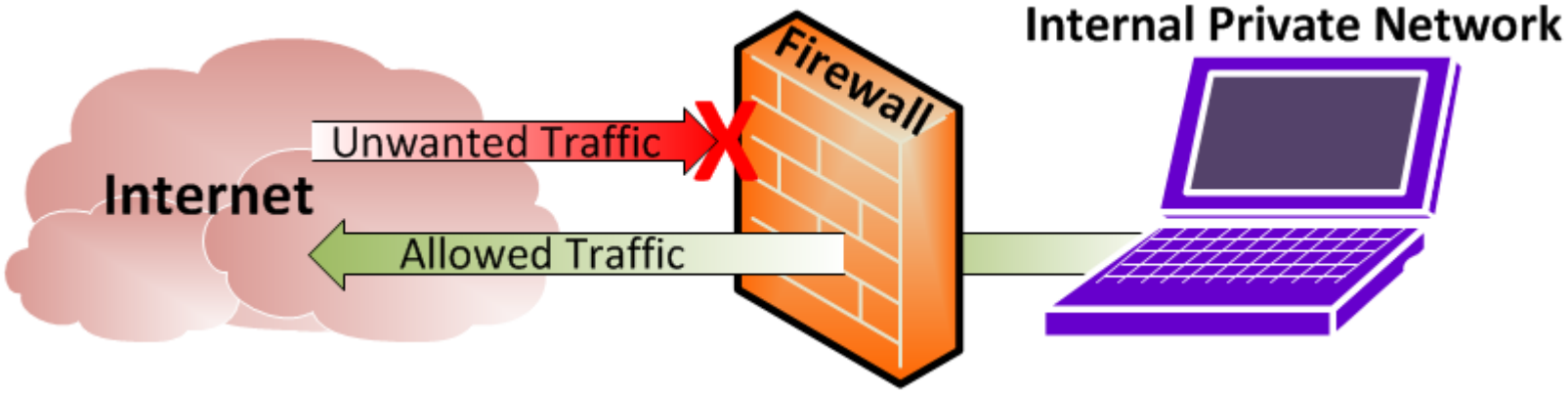
Encryption

Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information.

- An encryption key is a series of numbers used to encrypt and decrypt data. Encryption keys are created with algorithms. Each key is random and unique.
- There are two types of encryption systems: symmetric encryption and asymmetric encryption. Here's how they're different.
    - **Symmetric** encryption **uses a single password** to encrypt and decrypt data.
    - **Asymmetric** encryption **uses two keys** for encryption and decryption. **A public key**, which is shared among users, encrypts the data. **A private key**, which is not shared, decrypts the data.

Protection Mechanisms

Firewalls



- Prevents information from flowing between untrusted network (Internet) and trusted network (internal network)
- Various types available that include packet filtering, proxy, and stateful inspection
- Acts as a gatekeeper and operates based upon rule sets
- Use of both “Black” lists (i.e., exclusive) and “White” lists (i.e., inclusive) to heighten scrutiny of traffic

Protection Mechanisms

Anti-Virus (1 of 2)

A **computer virus** is code that when executed is designed to enter a computer and replicate itself. Viruses that are designed to harm a computer are classified as a type of "malware". The nefarious aims of different types of malware are wide-ranging, including but not limited to:

- Ransomware that encrypts sensitive files, photos and documents and other data on your computer, requiring you to make a payment (often via Bitcoin) to receive a password to decrypt and unlock these files.
- Trojan horses that enable a hacker to completely take over your computer and execute programs as if they were actually using your keyboard and mouse.
- Spyware that "mines" personal information from your computer, selling it off to the highest bidder.
- Adware that generates unintended pop-ups from shady advertisers.

Protection Mechanisms

Anti-Virus (1 of 2)

Anti-virus software provides protection against threats by performing key tasks:

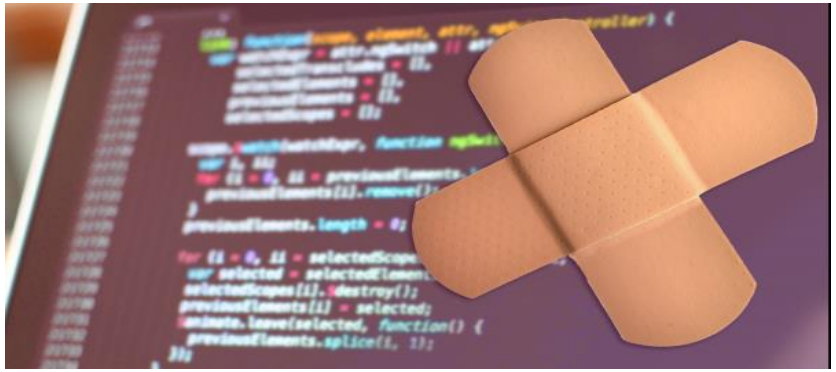
- Pinpointing specific files for the detection of malicious software
- Scheduling automatic scans
- Scanning either one file or your entire computer at your discretion
- Deleting malicious codes and software
- Confirming the safety of your computer and other devices

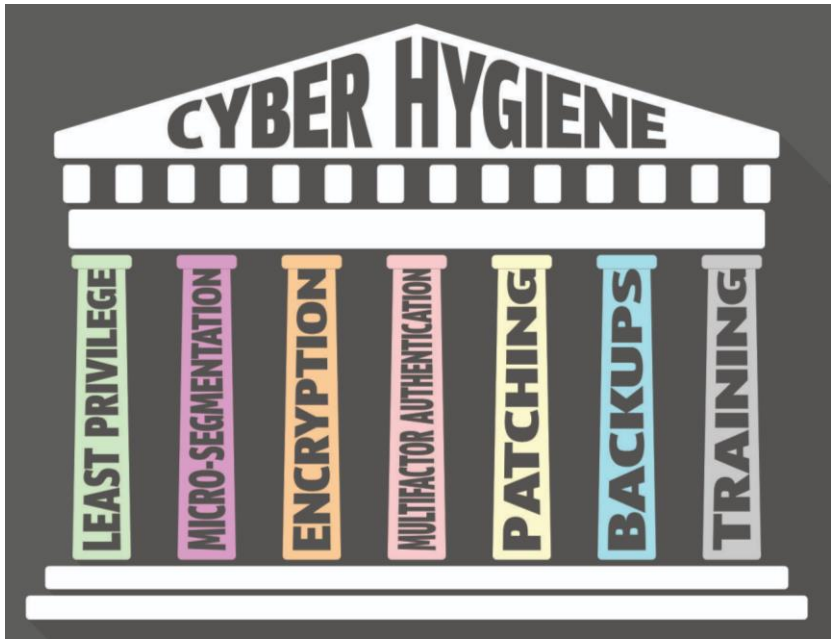
Protection Mechanisms

Software Patching/Cyber Hygiene

A software patch is a piece of code tailored to fix a bug, or to add new features in an application.

- **Patching** is a process to repair a vulnerability or a flaw that is identified after the release of an application or a software.
- Unpatched software can make a device a vulnerable target of exploits. Patching a software as and when the patch is released is critical to deny malware access. The consistent upkeep of patching and other network security measures is known as **cyber hygiene**.
- Patches mostly concern security while there are some patches that concern the specific functionality of programs as well. Patch Management is mostly done by software companies as part of their internal efforts to fix problems with the different versions of software programs and also to help analyze existing software programs and detect any potential lack of security features or other upgrades.
- Quick and instant responses to patch updates would mitigate the chances of data breaches that can cause due to unpatched software.





Module #2

Frameworks, Optics, and Models Used in Cybersecurity

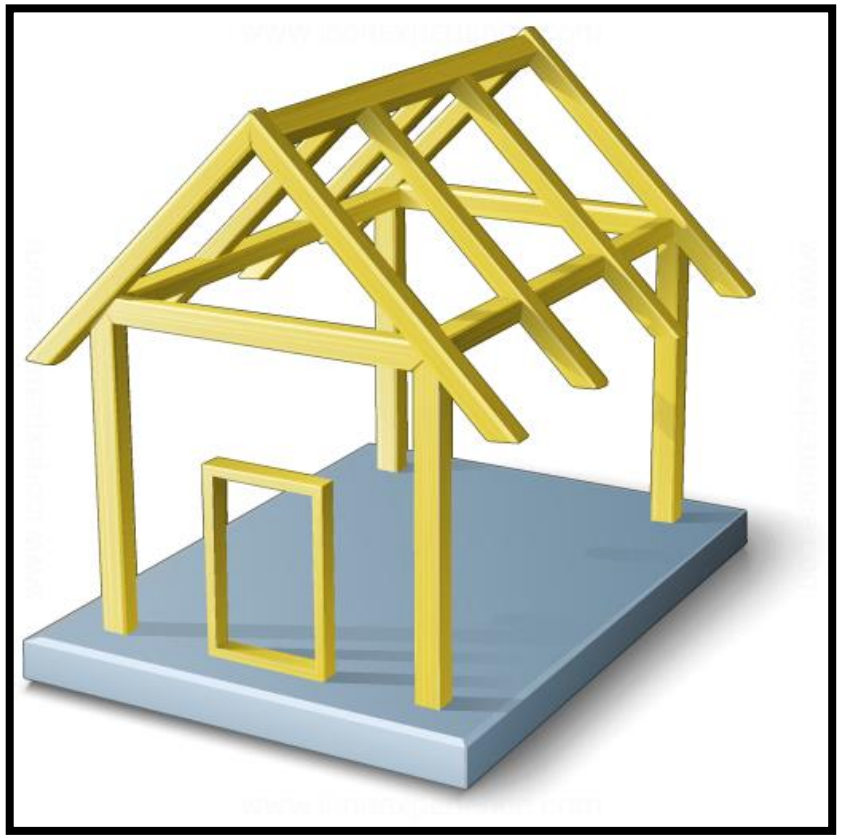
Frameworks, Optics, and Models

Examples of Models and Frameworks used in Cybersecurity

There are innumerable models and frameworks that can be used to bolster cybersecurity at an organization, agnostic of sector. These include:

- Center for Internet Security Critical Security Controls
- NIST Cybersecurity Framework (CSF)
- NIST Security Publications
- HIPAA Security Rule
- NIST CSF – HIPAA Cross Walk
- PCI Data Security Standard (DSS)
- Biba Integrity Models
- Bell-LaPadula (BLP) Confidentiality Model
- The Common Criteria (CC)
- Trusted Computing Base (TCB)
- Information Technology System Evaluation Criteria (ITSEC)
- Clark-Wilson Integrity Model
- Graham-Denning Access Control Model
- Harrison-Ruzzo-Ullman Model
- Brewer-Nash Model (Chinese Wall)
- The ISO 27000 Series

****Note: This list is by no means exhaustive, and represents just a small sample of frameworks and models for use depending on the nature of the enterprise being evaluated, the processes and network assets involved and, yes, the costs incurred in implementing recommended mitigations.*



Preferred Framework(s): The Cyber Threat Framework (CTF)

How are the Four Stages of the CTF Defined/Characterized?

LAYER 1 - STAGES				
PREPARATION	ENGAGEMENT	PRESENCE		EFFECT
Actions to prepare to conduct cyber activities	*Actions to gain unauthorized access*	*Actions to maintain unauthorized access*		*Outcomes of actions on targeted system*
LAYER 2 - STAGES				
Plan Activity	Deploy Capability	Establish Initial Control	Establish Persistence	Deny access
Research & Analysis	Interact with Target	Hide	Expand Presence	Alter System Behavior
Resource/Capability Development	Drive-by attacks	Refine Targeting		Extract data
Conduct Reconnaissance	Exploit Vulnerabilities			Destroy HW/SW/Data
Stage Capabilities	Deliver Payload			Enable Other Operations
Initiate Operations	Suspicious Network Activity			
LAYER 3 - STAGES				
Review Strategy	Deploy Electronically	Unauthorized access	Anti-intrusion Detection Measures	Disrupt/Degrade Links
Plan Mission	Physical Proximity	Automated Malware C2	Anti-forensic measures	Disrupt/Degrade Network
Issue Guidance	Credential Farming	Establish Communications	Monitor Administrators	DDoS
Gather Intelligence	Social Engineering	Network Mapping	Increase User Privileges	Install Ransomware
Identify Targets	SQL Injection	Software Packing	Lateral Movement	Create Botnet(s)
Develop Infrastructure	Masquerade	Masquerading	Identify Targets of Opportunity	Deface Websites
Physical Reconnaissance	Use of Exploit Kit	Obfuscate Payloads	Service Manipulation	Relocate/Store Data
Electronic Reconnaissance	Cross Site Scripting	Indicator Blocking	Registry Run Keys	Disclose Data
Stage Externally/Internally	Webmail Vulnerability	Scripting	BIOS Rootkit	Exfiltrate Data
Issue Operational Tasking	App Vulnerability	Disabling Security Tools	Master Boot Record	Establish C2 or Hop Point

Frameworks, Optics, and Models

Optic(s): *The view(s) one has of something; perspective*

Problem: A matter or situation regarded as unwelcome or harmful and needing to be dealt with and overcome.

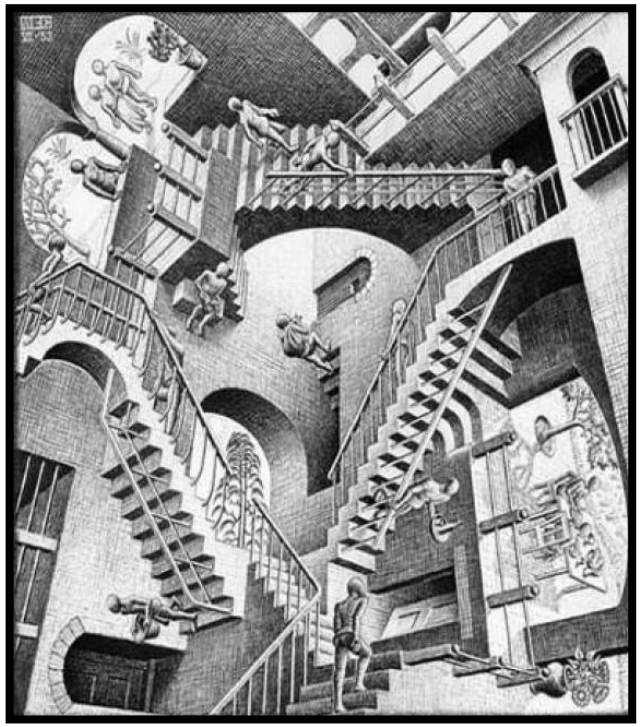
Problems have Solutions:

- Typically, such issues are localized; Direct and indirect variables can be identified easily.
- Requires a specific remedy; Perhaps even a higher "amount" of one already known.
- When addressed at an early stage, impacts can be greatly limited or mitigated, sometimes without a return of the issue; Monitors/limiters can be used to warn of problems in nascent stages or to keep problems from repeating.
- Typically, problems will present themselves before crises have occurred and, therefore, give cognizant personnel the chance to address shortcomings.

Crisis: A time of intense difficulty, trouble, or danger; A time when a difficult or important decision must be made.

Crises have Outcomes (Which Must be Managed):

- Typically, there are unpredictable cascading effects to crises which make them very difficult to contain; Variables act upon each other.
- Typically, a number of "smaller" solutions must be combined to control the effects of a crisis.
- Once a crisis has been acknowledged, a group effort is necessary to limit negative impacts and begin recovery; Ensuring a crisis is NOT repeated can be very expensive due to the monitoring of multiple "fault" points required.
- Typically, damage has already been done; A "triage" and "quarantine" posture is often required.



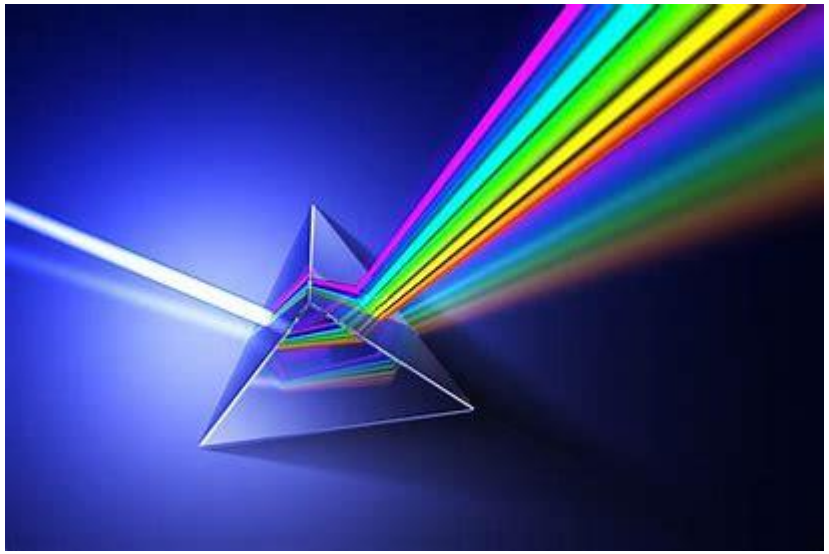
Bottom Line: Problems can be Resolved. Crises must be Managed!

Frameworks, Optics, and Models

Filter(s): *A device through which something is passed in order separate one substance from another*

Intelligence: the collection of actionable information which is both accurate and timely.

Accurate Intelligence is the key to desirable outcomes.



- The highest quality intelligence is integral to (1) determining whether an issue is a problem or a crisis, (2) forecasting what the potential impacts of that problem or crisis are and, subsequently, (3) giving proper weight to the cost-benefit analysis that will be used to justify how best to address the problem or crisis.
- The importance of accurate intelligence grows immensely when facing many issues concurrently, compared to just one issue.
- Initial reports of any event should NEVER be taken as the final state(s) or posture of the variables known to be involved; One must be able to "get ahead" of potential outcomes to halt them (hopefully, prior to fruition).
- The continuous collection of information, during an issue, for purposes of formulating operational intelligence is key. NEVER stop collecting intelligence. * (SWOT analysis)
- Intelligence MUST be binned into: (1) what is **believed**, (2) what is **assumed**, and (3) what is **known**. Higher levels of trust should be placed on incoming intelligence in that order.

  - ***Believe:*** *There is no underlying context, but experience or casual observation are used to explain the current situation.*
  - ***Assume:*** *There is "strong" underlying context, but the theory has yet to be proven for the current situation.*
  - ***Know:*** *Fact. Shown to be true for the current situation.*

Module #2

Group Project:

The Cybersecurity Assessment and Presentation

Cybersecurity Assessment

Group Project Working Documents: Starting Point

Each team will be given an enterprise profile and a list of the current operating environment, as seen below.

Team 9 – Charmin's Profile

Charmin is a regional cloud service provider that focuses primarily on providing hosted services to k-12 academic institutions and non-profits. The company is headquartered in San Diego, California and has clients in 14 states.

Industry: Cloud service provider

 # employees: 65

 # locations: 2

Public or privately held: Private

Types of data: employee and client records, intellectual property, strategic plans.

IT Infrastructure: Charmin uses a 3rd party provider for its client's data hosting needs.

- Hardware – Sophos firewalls; Cisco switches and routers; Apache web servers; Mix of vendors for laptops and desktops
- Software – Google G-Suite; QuickBooks

IT support model: Charmin employs 1 full time internal IT staff and primarily relies on its 3rd party data hosting provider for technical support and expertise.

Key vendors:

- Payroll – Paychex
- Insurance Broker – Willis Towers Watson
- Telecommunications – AT&T
- Security Monitoring – None (3rd party provider handles data center security)
- Physical Security – None (3rd party provider handles data center security)

Mobile device policy: Company does not provide mobile devices, strictly BYOD environment

Current Security Program Components

- Annual employee security awareness training
- Annual mock phishing exercise
- Annual IT security assessment

Current Operating Environment

1. A hurricane has knocked out power within the U.S state of Hawaii. Unfortunately, Hawaii is a hub for major telecommunications cross-continental cable landings spanning the Pacific Region, from Asia to the west coast of the United States. Some networks are reported to have been temporarily disrupted while others are completely inoperable.
2. A hacker by the name of "Nomad" claims to have hacked the payroll business Paychex. Although Paychex has not issued a public statement yet, there are some unofficial reports that thousands of client profiles containing personally identifiable information (PII) have been exfiltrated (or taken) by Nomad.
3. A recently terminated employee has threatened to file suit against the Charmin Company for prejudice. They now claim to have evidence of this prejudice that they were able to acquire from a roaming account which should have been disabled once they left.
4. The networks of a number of healthcare-related facilities around the world have been victimized by the latest version of the "IwannaEatIceCream" computer virus. The hackers are protesting the high cost yet low quality of some cancer treatments.
5. The company's IT deployment unit has reported that the new routers that were recently bought have a defect which does not allow them to be backwards compatible with the current Cisco routers being used.
6. A number of Western European countries have jointly passed new data privacy rules. The equipment to be purchased to comply with these new rules is expected to be financed entirely by network service providers.
7. The CEO's account has been hacked and important information on their computer has been encrypted by ransomware.
8. A thumb drive has gone missing from the company's IT service desk. A number of this fiscal year's employee evaluations - containing some PII - were saved on this drive.
9. Small riots have broken out in some parts of the United States after it was found that a hacker was able to change the prices of food at a U.S. national grocery chain, causing some prices to reach 20x what they were just three hours before.

Cybersecurity Assessment

Group Project Working Documents: Starting Point

Each team will also be provided with a template file which has fillable fields, such as the one shown below.

Affected Enterprise: _____

Step #1: Risk, Threat, Vulnerability Assessment

#	Issue(s)	P/C	A, B, or C

Organizational *(enterprise structure needed to conduct stated mission)*	Legal *(constraints and restraints on how stated mission is achieved)*
Cultural *(Daily application of IT hardware, software, and processes used to achieve stated mission within established constraints and restraints)*	Technological *(IT hardware, software, and processes used to achieve stated mission within established constraints and restraints)*

Cybersecurity Assessment

The Distinction between Organizational and Cultural Aspects of an Enterprise

Organizational component of an enterprise:

- Determines how the organization reacts to a situation given its management structure(s) and operating process(es).

Cultural component of an enterprise :

- Determines how people that make up the organization react to situations given rules that govern their behavior, both in and out of work.

For example, an enterprise creates software used in the armed forces of their host country. Although information and operational security are observed at the work site due to the sensitivity of the products manufactured, the employees of the enterprise are not hindered in belonging to social media groups centered on working for the enterprise. On the group's website, which has lax security, photos are posted, and names and job duties are provided, as well as locations where major celebrations take place. Although legal, the malalignment of on-duty and off-duty behavior might be questionable.

Cybersecurity Assessment

The reason(s) for this (and any) cybersecurity assessment

The GOAL, once again, is to achieve as high a level of Cybersecurity-related return-on-investment (ROI) as possible!!!

- **This is NOT the same as reaching optimal efficiency or effectiveness in security of enterprise network operations.**
- Ensures that resources are used with every unit of exchange (i.e., money, currency, good will, etc.) spent providing optimal value to as many parts of the host enterprise as possible.
- Ensures that the enterprise does not spend its hard-earned winnings or limited resources on building IT backend infrastructure and customer interfaces which are unnecessary for the competitive environment.
- Provides a way for leadership and management to justify expenditures and decisions that normally would be difficult to explain due to expense and/or exposure to risk.

Module #2

Affiliation/Situation:

The Lone Entrepreneur and Sole Employed

The Lone Entrepreneur and Sole Employed

Effective cybersecurity on a slim budget

“Do what you can, with what you have, where you are!”

- Theodore Roosevelt (26th American President, from 1901-1909)

What can **one single businessperson or entrepreneur** - working in isolation - do to vastly improve their own cybersecurity posture when resources are limited or even non-existent?

Assumptions made:

1. The entrepreneur has a web-enabled computer (i.e., tower unit, laptop, etc.) or mobile handheld device, as well as Internet connectivity.
2. The entrepreneur, whether voluntarily or involuntarily, has limited interactions with stakeholders (i.e., partners, customers, suppliers, etc.) outside of that achieved with their computer or handheld device.
3. There are very few, if any, resources to expend on optimal cybersecurity solutions.
4. The entrepreneur has intellectual property of some value (i.e., monetary, intrinsic, etc.) stored on their computer and/or requires the use of that particular device to function for the health of entrepreneur’s enterprise (i.e., data is non-transferable or data transfer is not desired, for any reason).

The Lone Entrepreneur and Sole Employed

Defending against the effects of ransomware (1)

Ransomware

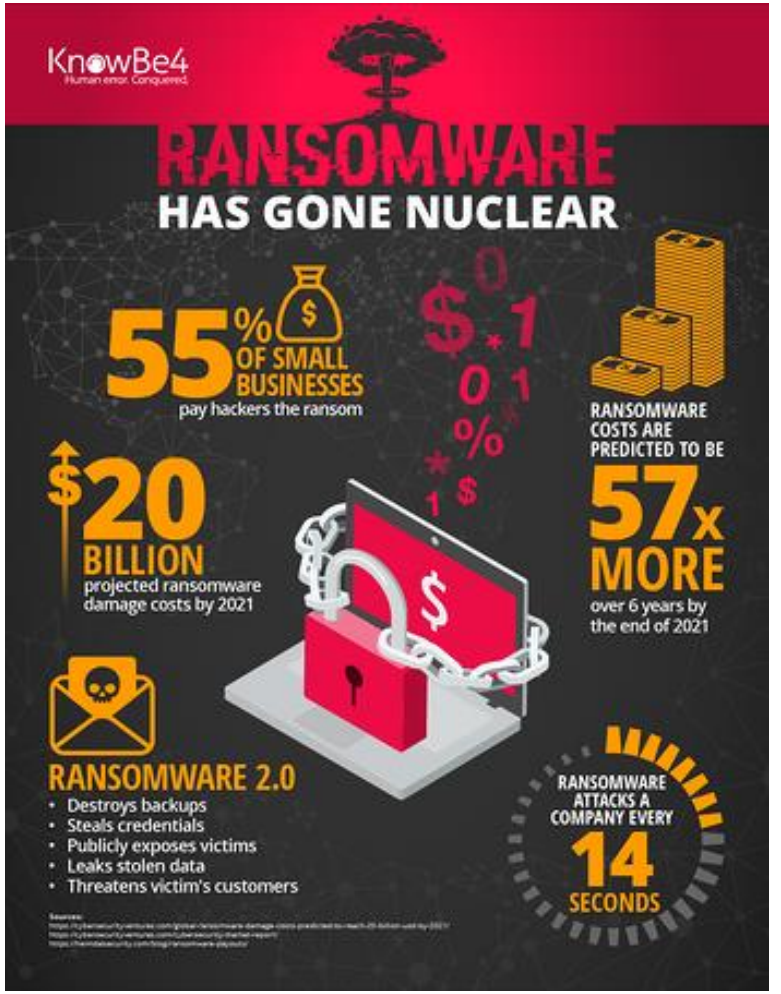
A type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

The Ransomware Crypto Economy

- There are at least two ways in which cryptocurrency is important for ransomware attacks. The first one is the most obvious — the majority of the ransoms paid during these kinds of attacks are generally in cryptocurrency. This was the case, for instance, in the WannaCry ransomware attacks, still the largest attack of its kind in history. Victims of the attack were instructed to send roughly $300 of Bitcoin (BTC) to their attackers.

- There is another way in which crypto and ransomware are intertwined, though. Today, plenty of hackers are offering "ransomware as a service," essentially letting anyone hire a hacker from online marketplaces. If you are so inclined, you can even buy ransomware off-the-shelf from these marketplaces. Both of these "services" can be paid for in — you've guessed it — cryptocurrency.

- Cryptocurrency is also implicated in many other forms of cyberattack. Cryptojacking — a form of attack that uses victim's computers to mine cryptocurrencies — is also on the rise, and new forms of malware such as Adylkuzz can be used by almost anyone with even a slight level of technical knowledge. Though these forms of attack are not technically ransomware, they further suggest the deep relationship between cryptocurrency and cybercrime.



The Lone Entrepreneur and Sole Employed

Defending against the effects of ransomware (2)

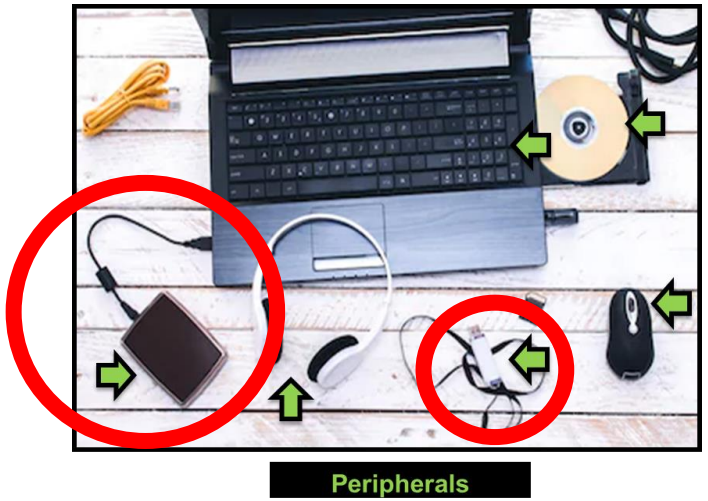
Peripherals

- A **peripheral device** (shown by the green arrows in the graphic) is defined as a computer device, such as a keyboard or printer, that is not part of the essential computer (i.e., the memory and microprocessor). These auxiliary devices are intended to be connected to the computer and used.
- Common external **peripheral devices** include (but are not limited to) devices like a mouse, keyboard, pen tablet, external hard drive, printer, projector, speakers, webcam, flash drive, media card readers, and microphone.

The Lone Entrepreneur and Sole Employed

Defending against the effects of ransomware (3)

The Mechanics: In most instances, the ransomware developer only encrypts what are likely important data files to induce pressure for the victim to pay (yellow arrow). The ransomware developer tends to leave the processors, operating systems, and peripherals (i.e., keyboard and mouse, etc.) operating to allow the desired payment to occur. However, when doing so, the developer may not have scripted their malware to disable any external drives (circled in red in the adjacent graphic) attached to the computer. (****Note: keeping the drive attached for long periods of time poses high risks and limits the benefits of what is otherwise a low-cost redundancy.)*



The Steps to Take to Lessen Risk: To take advantage of this cost-effective option for pre-empting the negative effects of a potential ransomware event, the drives should be attached to the computer and the data uploaded frequently enough so that any loss in data – from missing the very last file update if anything does occur to the computer - is minimal. ***Once these important files are updated, the drive should be quickly removed.*** Leaving the drive attached during a ransomware attack may still allow the user to detach the drive with the data safely saved, but the risk of these data being corrupted is now heightened. Only those files that are most important to the user should be saved on the external drive as attempts to save too much too often will also increase exposure. This practice is meant to spare a user the loss of ***THE MOST IMPORTANT FILES*** on their system and not as a complete memory back-up which may introduce greater risk exposure to the drives.

The Lone Entrepreneur and Sole Employed

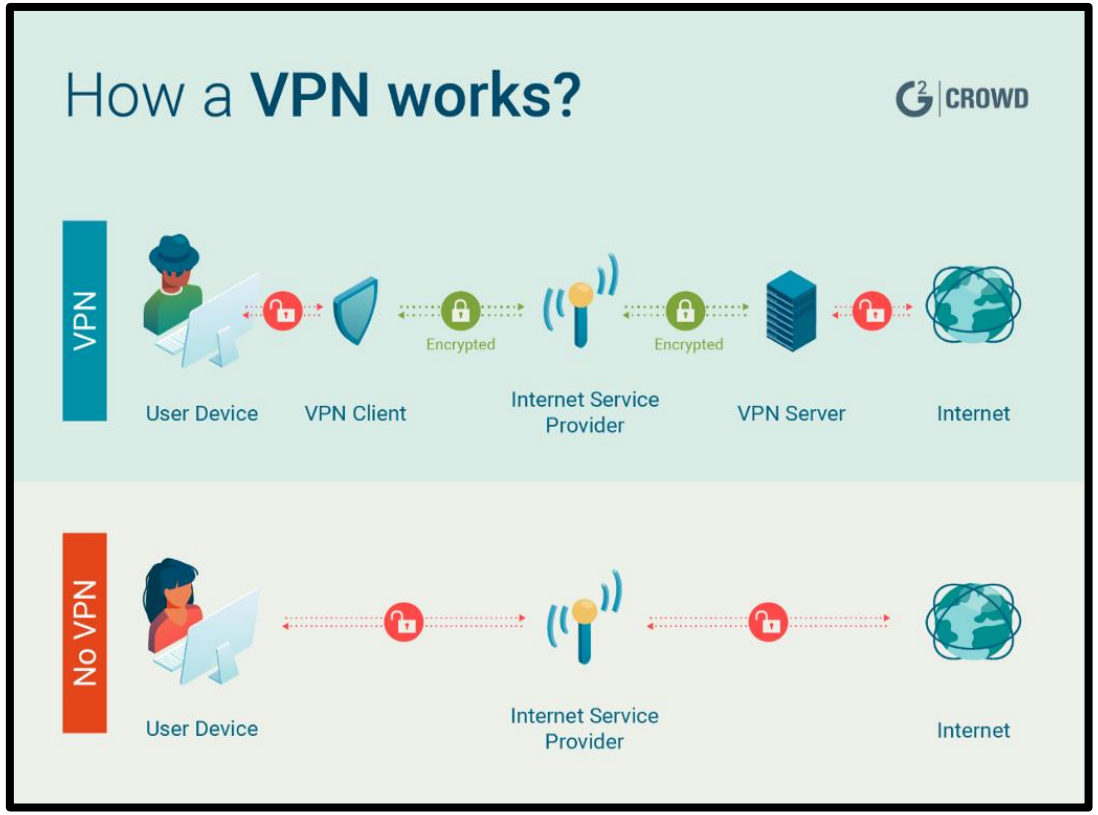
ZOOM!!!! . . . . Protecting your privacy!!!

Best practices for ensuring reliability and security of ZOOM calls

- Login policies: consider if using single sign-on (SSO) technologies such as Google or Okta is necessary to allow users to access Zoom.
- Password-protect all of your meetings, otherwise anyone will be able to join, which only increases the risk.
- Use the Waiting room feature - it will allow the meeting host to check each participant before letting them in.
- Disable the “Join before host” function to ensure the participants aren’t surprised by malicious actors
- Disable participant screen sharing to minimize the risk of meeting hijacking
- Lock meeting when everyone has joined
- Ensure you know which accounts have been inactive over the past month
- Monitor Windows UNC path sharing
- Monitor anomalous admin activities as well as new and deleted users
- Do not use Personal Meeting IDs
- Know about any admin control setting that are not being met
- Keep the Zoom client updated - install available updates immediately once they are released. Cybercriminals are more prone to attack the tool and Zoom acts accordingly - their latest update features password protection for all meeting by default.
- Keep track of relevant metrics related to your guests, such as which hosts create the meeting most often and for what number of guests, recent activities by guests, what meeting IDs are consistently being used by guests, who outside of your organization is joining meetings most often, foreign participants and where do they join from, etc.
- Do not share your meeting ID, as anyone will be able to join. The UK Prime Minister Boris Johnson highlighted this risk by showing the ID of his cabinet meeting to the entire world via his Twitter account - warn your employees to never copy this idea. Do not post public links to your meeting either.
- Keep track of your user activity, especially if they make changes to their user profiles, consistently use personal meeting rooms, or display anomalous behavior.

The Lone Entrepreneur and Sole Employed

Virtual Private Networks



A **virtual private network (VPN)** gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

The Lone Entrepreneur and Sole Employed

Virtual Private Networks

NSA Cybersecurity Advisory: Malicious Cyber Actors Leveraging VPN Vulnerabilities for Attack; Check VPN Products for Upgrade. Published October 07, 2019

The National Security Agency is alerting that multiple Advanced Persistent Threat (APT) actors are currently exploiting various VPN vulnerabilities to gain access to unprotected networks. Malicious cyber actors often use newly released software patches to develop exploits and access networks which have not yet upgraded with vendor released patches. Multiple VPN vulnerabilities have been published over the last six months affecting several major VPN products. Upgrade your VPN products to the latest vendor released versions to protect your networks from these attacks.

Known vulnerabilities include Pulse SecureTM, Palo Alto GlobalProtectTM, and Fortinet FortigateTM VPN products. If you suspect you may have been compromised:

- Immediately upgrade your VPN to the latest version;
- Reset credentials before reconnecting the upgraded devices to an external network;
- Review your network accounts to ensure adversaries did not create new accounts;
- Update VPN user, administrator, and service account credentials;
- Revoke and create new VPN server keys and certificates.

The Lone Entrepreneur and Sole Employed

Virtual Private Networks

NSA Cybersecurity Advisory: Malicious Cyber Actors Leveraging VPN Vulnerabilities for Attack; Check VPN Products for Upgrade.
Published October 07, 2019

VPN Common Vulnerabilities and Exposures (CVEs) being currently exploited include but may not be limited to:

- **CVE-2019-11510** and **CVE-2019-1153** which allow for remote arbitrary file downloads and remote code execution on Pulse Connect Secure and Pulse Policy Secure gateways;
- **CVE-2018-13379** which allows specially crafted HTTP requests to download system files on Fortinet Fortigate devices;
- **CVE-2019-1579** which allows remote code execution against Palo Alto GlobalProtect VPNs.

The MITRE CVE site may be accessed at the following URL: https://cve.mitre.org/.

NSA strongly encourages system owners to upgrade their applicable VPN products to the latest versions, and review all account activity for anomalous use of legitimate credentials that may have been gained from the unpatched VPN.
****Note: For further mitigation and VPN hardening guidance, please refer to this NSA advisory, the Canadian Centre for Cyber Security's VPN Alert, the UK National Cyber Security Centre's Alert and your vendor's security configuration best practices documents.*

The Lone Entrepreneur and Sole Employed

Social Engineering

6 Types of Social Engineering Attacks

1. Baiting

- This type of social engineering depends upon a victim taking the bait, not unlike a fish reacting to a worm on a hook. The person dangling the bait wants to entice the target into taking action.

2. Phishing

- Phishing is a well-known way to grab information from an unwitting victim. Despite its notoriety, it remains quite successful. The perpetrator typically sends an email or text to the target, seeking information that might help with a more significant crime.

3. Email Hacking and Contact Spamming

- It is in our nature to pay attention to messages from people we know. Some criminals try to take advantage of this by commandeering email accounts and spamming account contact lists.

4. Pretexting

- Pretexting is the use of an interesting pretext — or ploy — to capture someone's attention. Once the story hooks the person, the fraudster tries to trick the would-be victim into providing something of value.

5. Quid Pro Quo

- This scam involves an exchange — I give you this, and you give me that. Fraudsters make the victim believe it's a fair exchange, but that's far from the case, as the cheat always comes out on top.

6. Vishing

- Vishing is the voice version of phishing. "V" stands for voice, but otherwise, the scam attempt is the same. The criminal uses the phone to trick a victim into handing over valuable information.

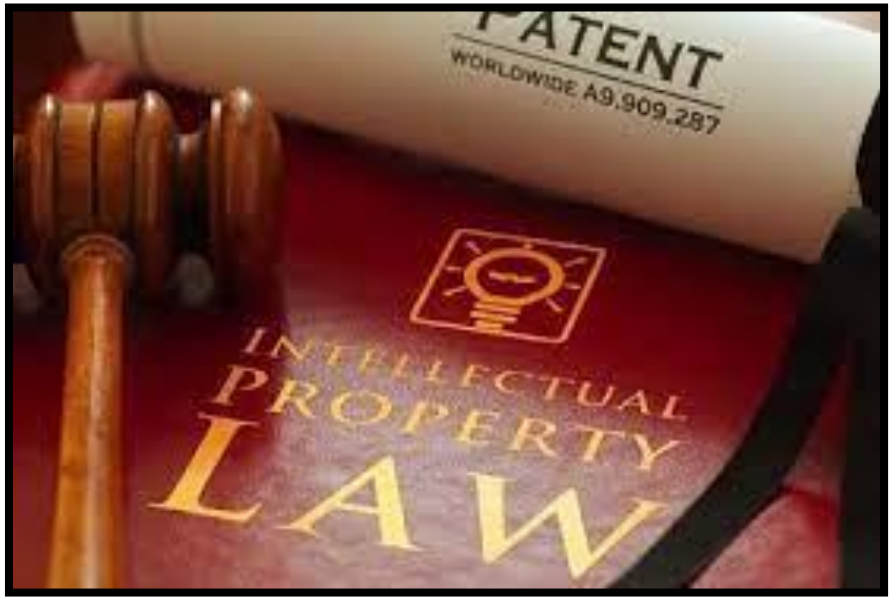
The Lone Entrepreneur and Sole Employed

Pre-emptive Legal Action: Ensuring your intellectual property remains yours

Provisional Application for Patent (United States)

A provisional patent application allows you to file without a formal patent claim, oath or declaration, or any information disclosure (prior art) statement.

- Since June 8, 1995, the United States Patent and Trademark Office (USPTO) has offered inventors the option of filing a provisional application for patent which was designed to provide **a lower-cost first patent filing in the United States and to give U.S. applicants parity with foreign applicants** under the GATT Uruguay Round Agreements.



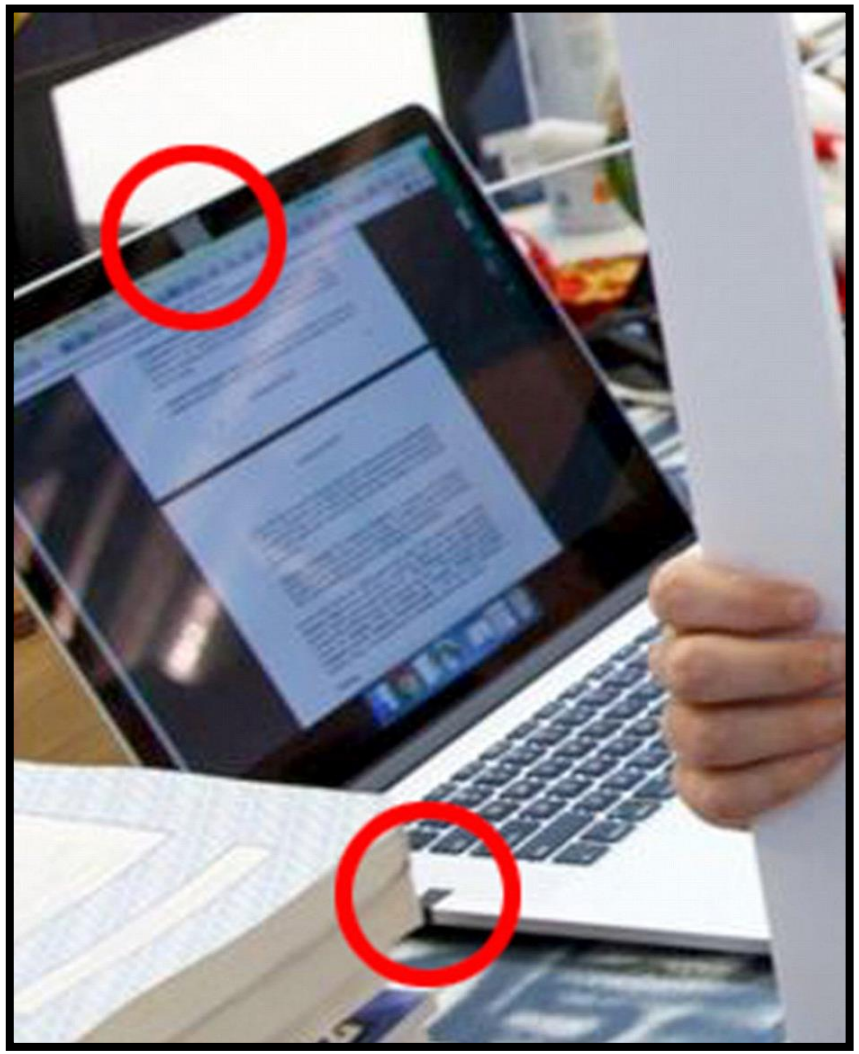
In other words, one might be able to file a relatively cheaper provisional application with USPTO to protect their intellectual property (i.e., important ideas in the form of files on your computer or any other web-enabled device) **for no more than 12 months.** A patent attorney should be consulted initially for optimal outcomes. (****Note: please peruse the regulations and laws outlined at the link provided in Course Documents.)*

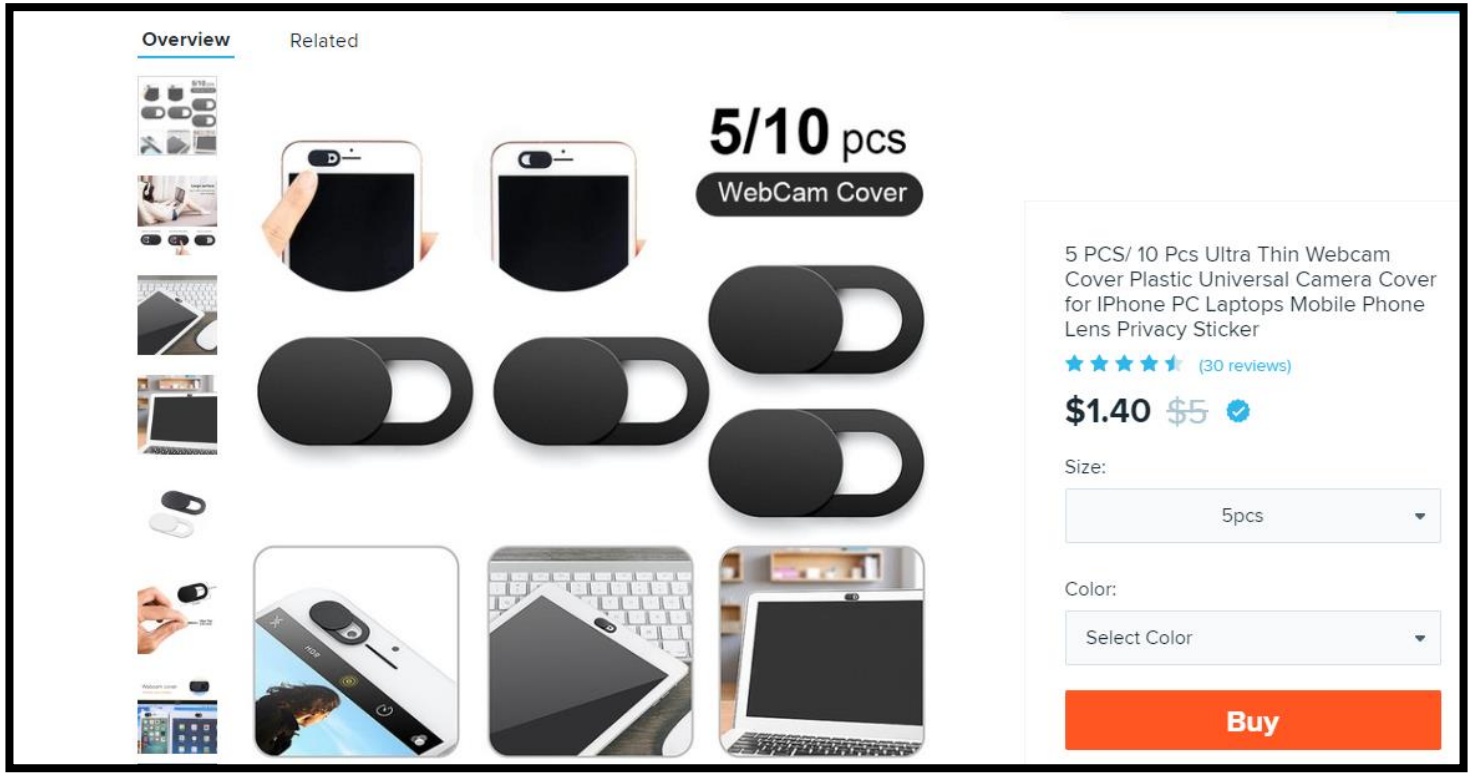
This could be an option for anyone who:

- 1. Has limited resources (like a sole employed/lone entrepreneur);
- 2. Has a great idea which happens to be saved on a digital device;
- 3. Has limited control over cyber threat defenses;
- 4. Has gauged that their idea will be completed within 12 months as to ensure the submission of a non-provisional patent application to maintain ownership.

The Lone Entrepreneur and Sole Employed

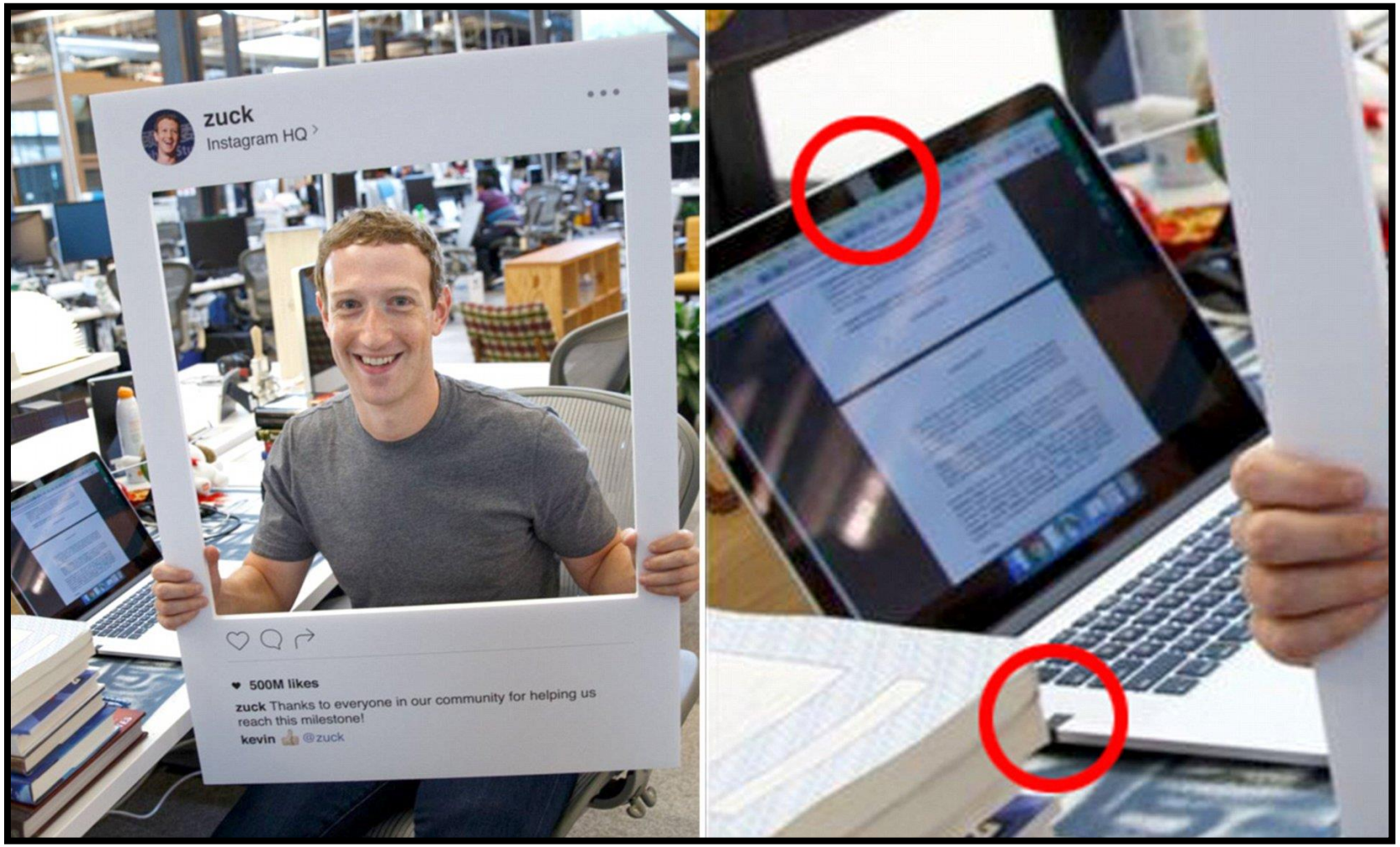
The camera on your web-enable device





The Lone Entrepreneur and Sole Employed

The camera on your web-enable device



The Lone Entrepreneur and Sole Employed

Operational Security, Communications Security, and Information Security

If only there were easily-accessible “pro tips” we could use to protect ourselves when going about our business matters and private lives in cyberspace such as on:

- Smartphones
- Home Wi-Fi Networks
- Traveling with Smartphones
- Facebook
- Facebook Mobile
- Twitter
- Instagram
- LinkedIN
- Keeping Kids Safe Online
- Photo Sharing
- Secure Chat

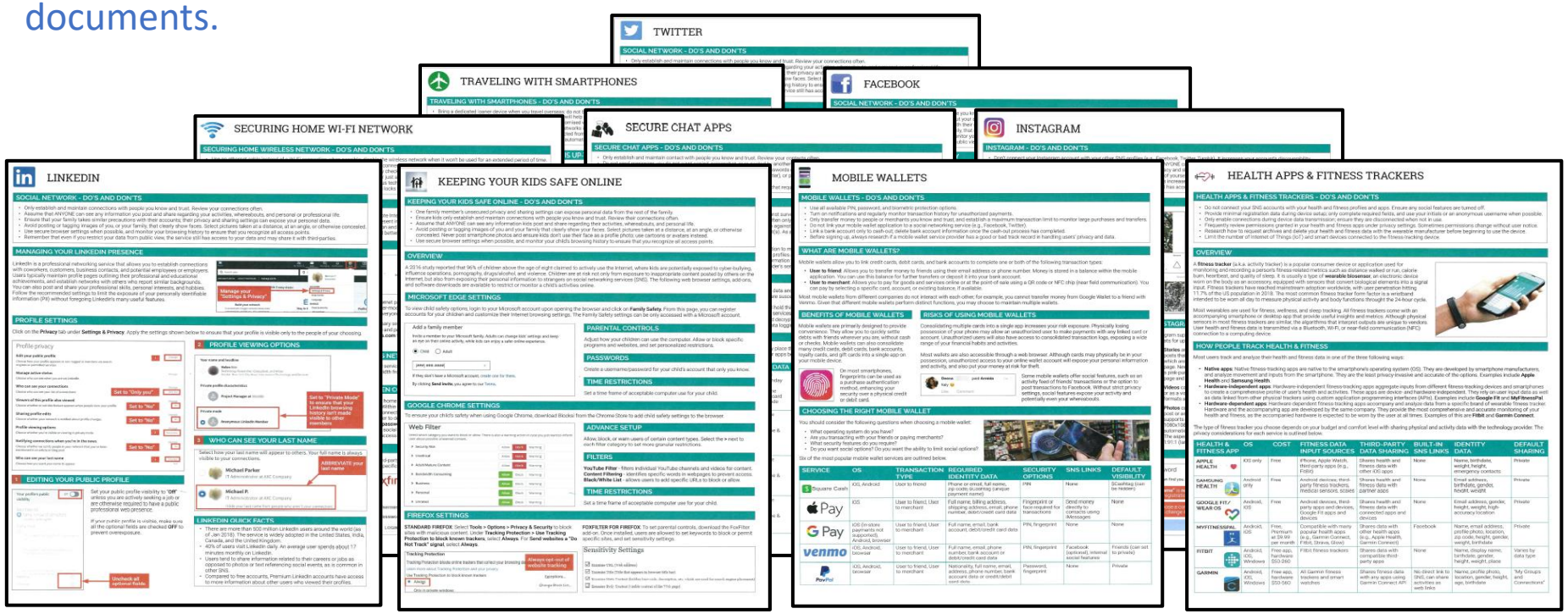
- EXIF Data Removal
- Mobile Wallets
- Health Apps & Fitness Trackers
- Online Registration
- Opting Out of Data Aggregators
- Identity Theft Prevention
- Voice Over internet Protocol (VoIP)
- Virtual Private Networks (VPN)
- Windows 10
- Online Dating Services
- Mobil Dating Apps

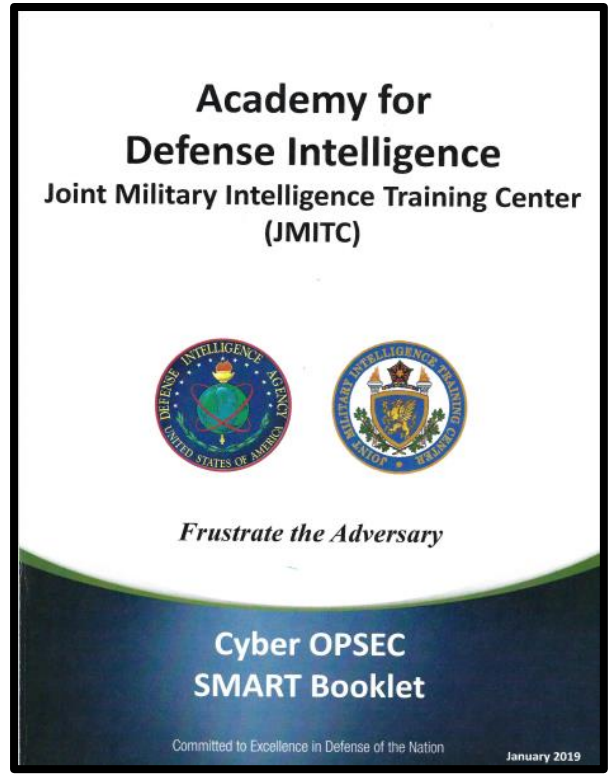
The Lone Entrepreneur and Sole Employed

Operational Security, Communications Security, and Information Security

Johns Hopkins University Carey Business School sought and received permission from the U.S. Department of Defense to disseminate the Joint Military Intelligence Training Center's Cyber OPSEC SMART Booklet (January 2019).

In it are approximately 50 pages of processes and instructions a user can follow to heighten that user's security of some of the most commonly used devices and online services globally, as well as take greater control over sensitive content. The booklet is located in your course documents.





JOHNS HOPKINS
CAREY BUSINESS SCHOOL

Introduction to Cybersecurity

Module #3

Today's Cybersecurity Job Market and Operating Environment • Affiliation/Situation: Small-to-Medium (SME) Enterprise • "Champions " of Cybersecurity • Planning for Contingencies: A Primer for the Basics • Planning for Contingencies: Business Impact Analysis (BIA) • Planning for Contingencies: Incident Response Plan (IR Plan) • Planning for Contingencies: Disaster Recovery Plan (DR Plan) • Planning for Contingencies: Business Continuity Plan (BC Plan) • Governance and Strategic Planning for Security • Developing the Security Plan • Developing Security Program Components: Implementing Security Education, Training, and Awareness (SETA) Programs

Module #3

Today's Cybersecurity Job Market and Operating Environment

Today's Cybersecurity Job Market and Operating Environment

The Cybersecurity Job Market!!!

- **According to the [US] Bureau of Labor Statistics, the number of individuals employed within the cyber security sector is slated to grow by 31% between 2019 and 2029. That rate far exceeds the average for all occupations.**
- **According to cybersecurity placement firm CyberVista, here is the breakdown of those new and continuing openings for cybersecurity jobs (in the United States) by industry as of April 2020:**
  - IT and Services: 103,001
  - Financial Services: 67,473
  - Computer Software: 66,341
  - Defense & Space: 49,708
  - Hospital & Health Care: 49,483
- **Cybersecurity jobs were already in high demand prior to the world turning upside down [due to the pandemic] with demand far outpacing supply [of applicants] to the tune of some 4 million open positions globally (as of April 2020), also according to Cyber Vista.**
- **More information on the nature of particular jobs within this field may be found at the following URL: https://www.neit.edu/blog/cyber-security-job-outlook.**

Sources:
https://www.secureworldexpo.com/industry-news/cybersecurity-job-market-2020-outlook
https://www.glassdoor.com/research/job-market-report-march-16/
https://www.cybervista.net/cybersecurity-jobs-pandemic/

Today's Cybersecurity Job Market and Operating Environment

Certifications : Where to begin? Where to focus? Which are the best? (*Answer to all: It Depends!) (I)*

Top-Paying IT Certifications in the United States

- Certified Information Security Manager (CISM) - $146,730
- Certified Information Systems Security Professional (CISSP) - $143,501
- IT Service Management (ITSM) - $130,215
- AWS Certified Developer - $127,358
- Certified ScrumMaster - $126,333
- Project Management Professional (PMP) - $126,281
- AWS Certified Solutions Architect - $125,214
- Certified Ethical Hacker (CEH) - $123,524
- Cisco Certified Network Professional (CCNP) - $121,082
- Agile and Scrum - $120,917
- Microsoft Certified Solutions Expert (MCSE) - $115,528
- Information Technology Infrastructure Library (ITIL) - $115,464
- Cisco Certified Network Associate (CCNA) - $101,254
- Microsoft Certified Professional (MCP) - $99,550
- CompTIA Security+ - $93,987
- CompTIA Network+ - $82,656
- CompTIA A+ - $78,629

Source: CompTIA; DOI: March 2021; found at https://www.comptia.org/blog/top-paying-it-certifications

**Note: CompTIA is a trusted source for IT-sector, education-related information. However, everyone should do their own due diligence to ensure that information they use to make impactful decisions is as current and relevant to their individual operating environment or living situation as possible.*

Today's Cybersecurity Job Market and Operating Environment

Certifications : Where to begin? Where to focus? Which are the best? (*Answer to all: It Depends!) (II)*

Top-Paying IT Certifications Globally

- Google Certified Professional Cloud Architect — $175,761
- AWS Certified Solutions Architect – Associate — $149,446
- CISM – Certified Information Security Manager — $148,622
- CRISC – Certified in Risk and Information Systems Control — $146,480
- PMP® – Project Management Professional — $143,493
- CISSP – Certified Information Systems Security Professional — $141,452
- CISA – Certified Information Systems Auditor — $132,278
- AWS Certified Cloud Practitioner — $131,465
- VCP6-DCV: VMware Certified Professional 6 – Data Center Virtualization — $130,226
- ITIL® Foundation — $129,402
- Microsoft Certified: Azure Fundamentals — $126,653
- Microsoft Certified: Azure Administrator Associate — $125,993
- CCA-N: Citrix Certified Associate – Networking — $125,264
- CCNP Routing and Switching — $119,178
- CCP-V: Citrix Certified Professional – Virtualization — $117,069

Source: Global Knowledge; DOI: February 2020; found at https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/#gref

**Note: Global Knowledge is a trusted source for IT-sector, education-related information. However, everyone should do their own due diligence to ensure that information they use to make impactful decisions is as current and relevant to their individual operating environment or living situation as possible.*

Today's Cybersecurity Job Market and Operating Environment

Certifications: Key Considerations

- **Certifications frequently carry heavier weight than degrees!!!!**
- **Research the following variables associated with each certification in which you have an interest:**
  - Training costs
  - Time to obtain
  - Marketability
  - Specialization vs. General Practice is also a consideration
- **Suggested guidance on certifying:**
  - Look at job postings for common requirements and certifications sought;
  - Find an institution (and/or texts) which provide(s) the knowledge you need to get the cert you want;
  - Decide on a deadline of completion for certifying;
  - Start planning your study and work schedule (for that duration) accordingly;
  - Focus on your goal(s)!

Easy Starting Points for Those Seeking Certifications!

CEH
- Provides insights into assessing the security of computer systems by using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner.

Network+
- Provides solid foundation of basic telecommunications principles and technology.

Security+
- Provides solid foundation of basic security principles and technology.

A+
- Provides entry-level technical knowledge on the servicing of PC computers to include installing, maintaining, customizing, and operating various functionality.

All are fine, relatively inexpensive starting points!

Module #3

Affiliation/Situation: Small-to-Medium (SME) Enterprise

“Champions “ of Cybersecurity

Affiliation/Situation: The Small-to-Medium Enterprise Employee

Effective Cybersecurity in an Organization

"Talent wins games, but teamwork and intelligence win championships."

- Michael Jordan (Famous US Basketball Player (Retired), 1986-2002)

How can someone - working in an organization – maintain and improve their own cybersecurity posture as well as heighten their colleagues' postures in a dynamic environment?

Assumptions made:

1. The SME employee is using the assets of the organization to which they are affiliated; This includes a web-enabled computer (i.e., tower unit, laptop, etc.) or mobile handheld device, as well as Internet connectivity, as well as accesses to the organization's sensitive internal networks.
2. The employee has online interactions with stakeholders (i.e., partners, customers, suppliers, etc.) via their computer or handheld device.
3. There are more resources to expend, relative to when one is a lone entrepreneur, on cybersecurity.
4. The enterprise has intellectual property of some value (i.e., operational, monetary, conceptual, etc.) stored on their information networks and requires some measured level of security to ensure operations go unhindered and to maintain reputational health.

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

Chief Executive Officer (CEO)

- Responsible for the day-to-day oversight of an entire organization.
- Responsible for setting budgets, deciding in which markets to compete, which product or service lines to develop, etc.
- The CEO can delegate tasks but NOT necessarily responsibility.
  - ****Note: Greater numbers of regulations germane to the handling and security of information are holding the CEO responsible for ensuring the organization practices due care and diligence.*
  - ****Note: Personal liability aimed towards decision makers such as the CEO is the reason why security budgets continue to increase.*

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

Chief Information Officer (CIO)

- Responsible to either the CEO or CFO on issues regarding the strategic use and management of information systems and technology within the enterprise.
- Previously, responsible for day-in, day-out technology operations, but due to greater enterprise dependency on technology they are NOW seen informing decisions on business-process management, revenue generation, and business strategy realization.
- This position bridges both the technology sphere and business world as a matter of position more than any other enterprise officer.

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

Chief Security Officer (CSO)

- Responsible for undertaking the risks that the enterprise faces and for mitigating these risks at levels which are deemed acceptable.
- Responsible for understanding the underlying foundations of how the enterprise operates and then creating and maintaining a security program that supports these critical activities.
- Provides overall security, ensuring enterprise compliance with applicable laws and regulations, and the meeting of security needs of customers, and security in alignment with the enterprise’s contractual obligations.

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

Chief Privacy Officer (CPO)

- A newer position, created due to the increasing demands on organizations to protect ever-growing lists of data and information.
- Oversees how the organization may document how privacy data is collected, used, disclosed, archived, and destroyed.
- Must understand the privacy, legal, and regulatory requirements with which the organization must comply.
- May be responsible for reviewing the data security and privacy practices of external stakeholders such as suppliers, partners, and other third parties, to ensure the host enterprise’s data continues to be protected outside of established internal measures.
- ****Note: **Privacy*** is different from ***security***. Privacy indicates the amount of control a person/entity has over their own information. Security refers to the measures taken to provide that control.

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

Chief Information Security Officer (CISO)

- Responsible for establishing communications/IT security strategy and ensuring data assets are protected.
- “Guardians of Information Security”; Their role is to create a strategy that deals with ever-increasing regulatory complexity, creating the policies, security architecture, processes and systems that help reduce cyber threats and keep data secure.
- Compliance is a key element of the role, as is understanding risk management.
- Must understand how the cybersecurity threat landscape is evolving and how that could affect the security risks facing their particular organization.
- They continually take account of everything from the risk of malware and hacking through to insider threats or unpatched vulnerabilities in the organization's systems.
- The CISO will likely take a key role in any incident response if there is a data breach.

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

CISO Stats

- Cybersecurity Ventures forecasts that 100 percent of large corporations (Fortune 500, Global 2000) globally will have a CISO or equivalent position by [end of] 2021 (up from 70 percent in 2018), although many of them will be unfilled due to a lack of experienced candidates.
- The second-highest paying tech job in 2019 is a CISO, with a salary range of $175,000 to $275,000. Fortune 500 corporations in big cities pay as much as $380,000 to $420,000 annually, and more, to their CISOs, much higher than the average range for the position in mid-sized companies, government agencies, and academia. At the top of the cybersecurity food chain (ranked by pay), there are a small number of CISOs earning 7-figure annual pay packages.
- The importance of cybersecurity is such that the vast majority (89%) of CISOs are regularly summoned by the board of directors to provide recommendations for the business, reports 451 Research and security firm Kaspersky.
- More than half (54%) of CISOs responding to consultant KPMG and recruiter Harvey Nash's 2019 IT leadership survey said they are a member of the operational board or executive management committee.
- Almost half (43%) of CISOs feel that they are in direct competition with other business and IT initiatives for funding, reports 451 Research and Kaspersky.
- But while 40% of CISOs say their organization has been subjected to a security attack in the past two years, just 29% of CISOs believe they're very well-positioned to deal with security risks, according to KPMG and Harvey Nash.
- Almost three-quarters (74%) of CISOs say the relationship between security and marketing is, at best, neutral, if not mistrustful or non-existent.
- More than half (57%) say their relationship with finance, on which they depend on for budget authorization, is strained.
- The vast majority of CISOs (88%) remain moderately or tremendously stressed, according to research from Nominet.

Sources: https://www.zdnet.com/article/what-is-a-ciso-everything-you-need-to-know-about-the-chief-information-security-officer/; CISO 500 Demographic Study Announced By Cybersecurity Ventures

“Champions” of Cybersecurity

Common Information Security Roles in Organizations

Data Handlers/Stakeholders

- **Data Owner**: Typically, a supervisor/manager in charge of a business function or unit, ultimately responsible for the protection of a specific subset of data or information.
- **Data Custodian**: Also, responsible for the protection of data via maintaining security controls; performing periodic back-ups; restoring data from back-ups; periodically validating the integrity of the data.
- **Data Analyst**: Responsible for storing the data in a manner which makes sense based on how the enterprise and users who must use it can access it immediately.
- **Data User**: Any individual who routinely uses the data to perform their work.

Module #3

Planning for Contingencies:

A Primer for the Basics

Planning for Contingencies

Introduction to Contingency Planning: Four Major Components

Systematic approaches to identify, contain, and resolve any unexpected adverse events and to plan for when – not if – defenses are compromised

- **Business Impact Analysis (BIA)**
  - Based upon threat/risk assessment and critical systems analysis
- **Incident Response Plan (IR Plan)**
  - Focuses on immediate response
- **Disaster Recovery Plan (DR Plan)**
  - Focuses on rapid recovery of critical systems
- **Business Continuity Plan (BC Plan)**
  - Focuses on maintaining business processes and systems

Planning for Contingencies

Contingency Planning – Recommended NIST Steps

NIST provides the following in the form of guidance for contingency planning (CP):

1. Develop CP Policy statement
2. Conduct the BIA – identify and prioritize systems
3. Identify preventive controls
4. Create contingency strategies
5. Develop contingency plan
6. Ensure plan testing, training and exercises
7. Ensure plan maintenance – validate annually

Module #3

Planning for Contingencies:

Business Impact Analysis (BIA)

Planning for Contingencies

Introduction to Contingency Planning: Business Impact Analysis (BIA)

Business Impact Analysis (BIA)

- A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.
- Potential loss scenarios should be identified during a risk assessment.
- Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries.
- There are many possible scenarios which should be considered.

The BIA should identify the operational and financial impacts resulting from the disruption of business functions and processes. Impacts to consider include:

- Lost sales and income
- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans

Source: https://www.ready.gov/business-impact-analysis

Planning for Contingencies

Contingency Planning: Time to Recovery Key Terms

Commonly-used time-based metrics for measuring relative success in recovery:

- **Maximum tolerable downtime**
  - Example: payroll system – 10 days
  - Example: email platform – 2 hours
- **Recovery point objective**
  - Typically measured in hours or days
- **Recovery time objective**
  - Typically measured in hours
- **Work recovery time**
  - Tied directly to recovery options

*Note: It should be remembered that time-based metrics will differ amongst all enterprises based on - but not limited to - the nature of the enterprise (e.g., commercial, industrial, security-related, utility, etc.), the enterprise's charter (i.e., why it exists), complexity of the processes involved (e.g., ease in rerouting of services, etc.), and de-confliction of efforts (with others' efforts) particularly during a crises situation.

Module #3

Planning for Contingencies:
Incident Response Plan
(IR Plan)

Planning for Contingencies

Introduction to Contingency Planning: Incident Response Plan (IR Plan)

Incident Response Plan (IR Plan)

- The aim of incident response is to identify an attack, contain the damage, and eradicate the root cause of the incident. An incident can be defined as any breach of law, policy or unacceptable act that concerns information assets, such as networks, computers, or smartphones.
- When your organization responds to an incident quickly it can reduce losses, restore processes and services, and mitigate exploited vulnerabilities. An incident that is not effectively contained can lead to a data breach with catastrophic consequences. Incident response provides this first line of defense against security incidents, and in the long term, helps establish a set of best practices to prevent breaches before they happen.

Optimal Management of Incident Response Should Include three elements:

1. A Comprehensive Plan

An incident response plan should prepare your team to deal with threats, indicate how to isolate incidents and identify their severity, how to stop the attack and eradicate the underlying cause, how to recover production systems, and how to conduct a post-mortem analysis to prevent future attacks.

2. The Right People in Place

Recruit the following roles for your incident response team: incident response manager, security analyst, IT engineer, threat researcher, legal representative, corporate communications, human resources, risk management, C-level executives, and external security forensic experts. Let all employees know what their responsibilities will be in the event of an attack.

3. [The Right] Tools

[There are] tools which handle security incidents on a large scale, instead of investigating one issue at a time. These tools analyze, alert about, and can even help remediate security events which could be missed due to insufficient internal resources.

Source: https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/

Planning for Contingencies

Security Incident Containment Strategies

For the purpose of immediate containment and heightening of one's control over outcomes during an information network security incident, it is recommended that the affected individual or enterprise should:

1. Disable compromised user accounts;
2. Reconfigure firewall to block problem traffic;
3. Disable compromised process(es) or service(s);
4. Disconnect affected network or network segment;
5. Power down computers and network devices

Planning for Contingencies

Information Security (InfoSec) Incident Recovery Process

Generally, an InfoSec incident recovery process will include the following steps:

1. Identify the vulnerabilities that allowed incident to occur
2. Address safeguards that failed
3. Evaluate monitoring capabilities
4. Restore data from backups
5. Restore services and processes
6. Continuously monitor system
7. Restore confidence of organization

Planning for Contingencies

Digital Forensics Methodology

Regarding digital forensic investigation of any security (likely InfoSec) incident, it is recommended that those leading do the following:

1. Identify relevant items of evidentiary value
2. Acquire (seize) the evidence without alteration or damage
3. Maintain evidence chain of custody
4. Analyze data without risking modification or unauthorized access
5. Report the findings to the proper authority/stakeholder(s)

Module #3

Planning for Contingencies:

Disaster Recovery Plan

(DR Plan)

Planning for Contingencies

Introduction to Contingency Planning: Disaster Recovery Plan (DR Plan)

Disaster Recovery Plan (DR Plan)

What do you when your information technology stops working?

- An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan.
- Priorities and recovery time objectives for information technology should be developed during the business impact analysis.
- Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. **A plan for data backup and restoration of electronic information is essential.**

Source: https://www.ready.gov/business/implementation/IT

Module #3

Planning for Contingencies:

Business Continuity Plan

(BC Plan)

Planning for Contingencies

Introduction to Contingency Planning: Business Continuity Plan (BC Plan)

Business Continuity Plan (BC Plan)

When business is disrupted, it can cost money. Lost revenues plus extra expenses means reduced profits. Insurance does not cover all costs and cannot replace customers that defect to the competition. A business continuity plan to continue business is essential.

Development of a business continuity plan includes four steps:

- Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement to recover critical business functions and processes.
- Organize a business continuity team and compile a business continuity plan to manage a business disruption.
- Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Following an incident that disrupts business operations, resources will be needed to carry out recovery strategies and to restore normal business operations. Resources can come from within the business or be provided by third parties. Resources include:

- Employees
- Office space, furniture and equipment
- Technology (computers, peripherals, communication equipment, software and data)
- Vital records (electronic and hard copy)
- Production facilities, machinery and equipment
- Inventory including raw materials, finished goods and goods in production.
- Utilities (power, natural gas, water, sewer, telephone, internet, wireless)
- Third party services

Source: https://www.ready.gov/business-continuity-plan

Planning for Contingencies

Business Continuity Strategies

Geo-location Options:

- **Cold site** – no hardware or peripherals
- **Warm site** - partially configured computing facility that includes all services, communications, and physical plant
- **Hot site** – fully configured computing facility that includes all services, communications, and physical plant
- **Mutual agreement** – two organizations serve as each others backup
- **Rolling mobile site** – outside organization provides mobile facilities
- **Service bureau** – service agency provides BC facility for a fee

Warning

The following images display destruction and human tragedy as witnessed and captured during the 9-11 terrorist attacks, specifically upon New York City.

Planning for Contingencies

Business Continuity Strategies

New York City, USA - September 10, 2001

Planning for Contingencies

Business Continuity Strategies

New York City, USA - September 10, 2001

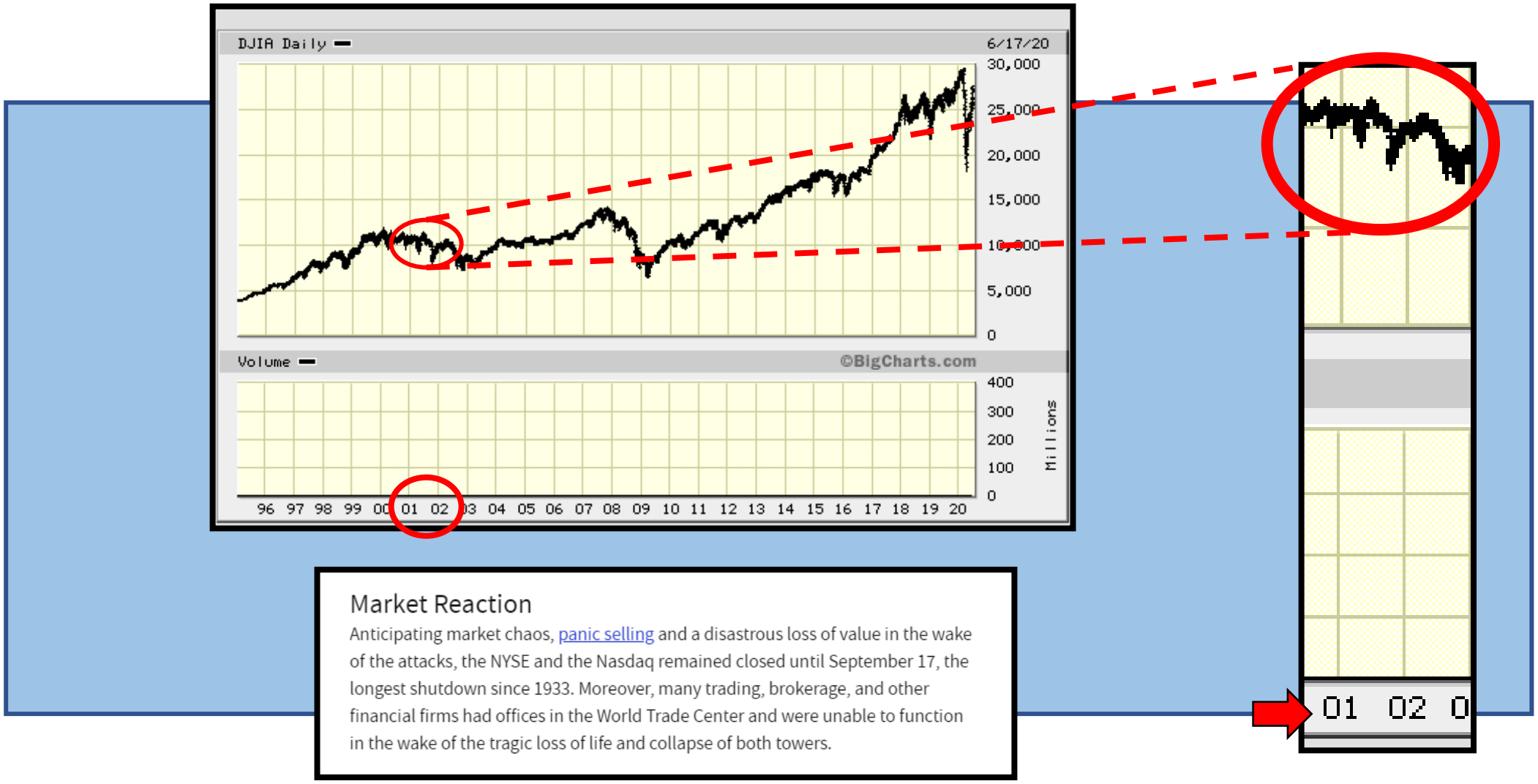
New York City, USA - September 11, 2001

Planning for Contingencies

Business Continuity Strategies

Planning for Contingencies

Business Continuity Strategies

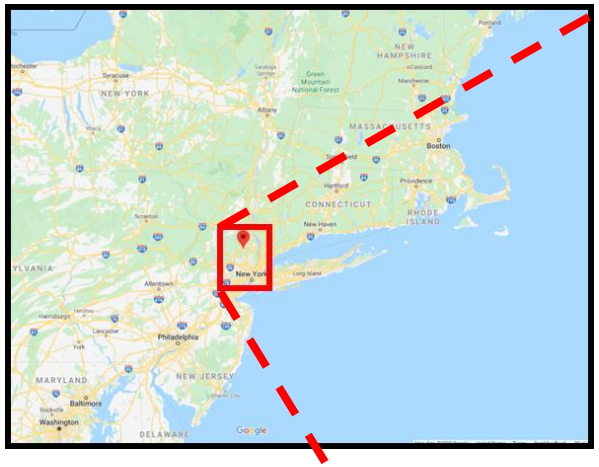


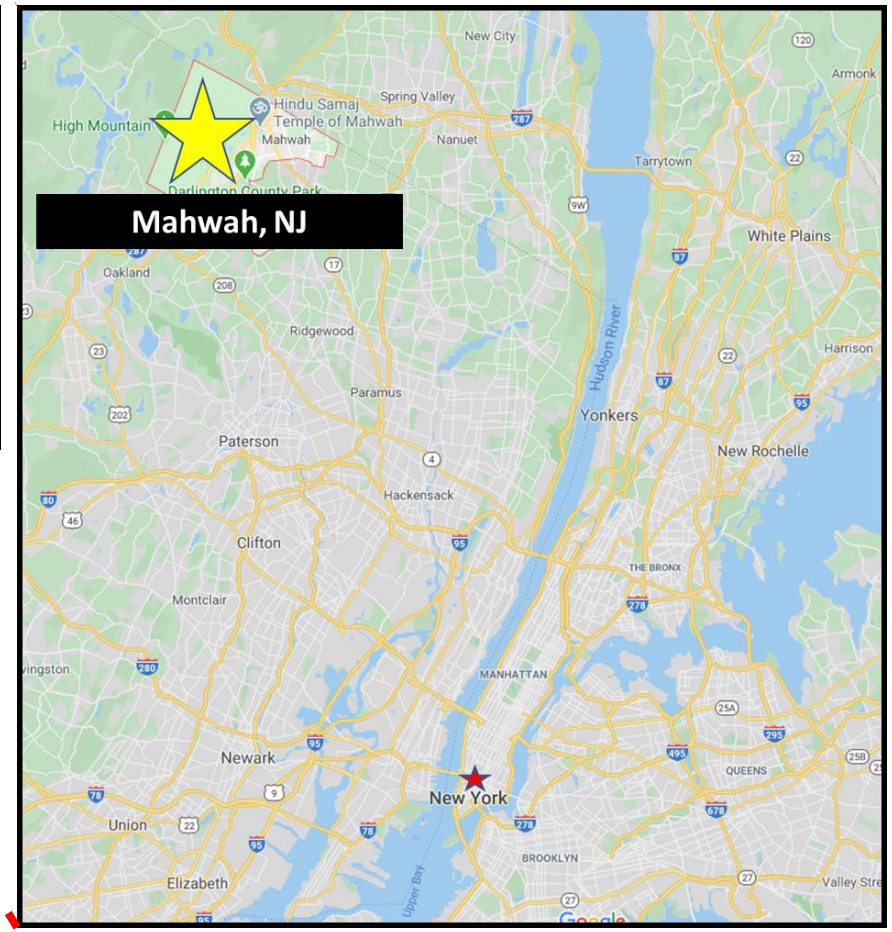
Market Reaction

Anticipating market chaos, panic selling and a disastrous loss of value in the wake of the attacks, the NYSE and the Nasdaq remained closed until September 17, the longest shutdown since 1933. Moreover, many trading, brokerage, and other financial firms had offices in the World Trade Center and were unable to function in the wake of the tragic loss of life and collapse of both towers.

Planning for Contingencies

Business Continuity Strategies





Planning for Contingencies

Business Continuity Strategies

The NYSE Euronext data center in Mahwah, New Jersey serves as a bridge between the New York Stock Exchange's history as the nation's oldest trading floor, and a future in which the majority of trading volume will be driven by computers. The halls of the facility are lined with street signs bearing the names of streets in downtown Manhattan, which provide a connection between Wall Street and the data center, and also create a navigational grid for staff within the 400,000 square foot building.

The facility features 60,000 square feet of colocation space for low-latency trading by hedge funds and investment firms, and industrial strength power and cooling infrastructure to ensure that the facility offers "always on" connectivity.

Source: https://www.datacenterknowledge.com/closer-look-nyse-euronexts-nj-data-center

Upper-left photo: The long main hallway of the NYSE Euronext data center provides a sense of the immense scale of the 400,000 square foot facility in New Jersey.

Module #3

Governance and Strategic Planning for Security

Governance and Strategic Planning for Security

Strategic Planning

Information security (InfoSec) must support strategic plans of all business units (BU)

- InfoSec strategic plan cannot be developed in a vacuum

Key BU considerations:

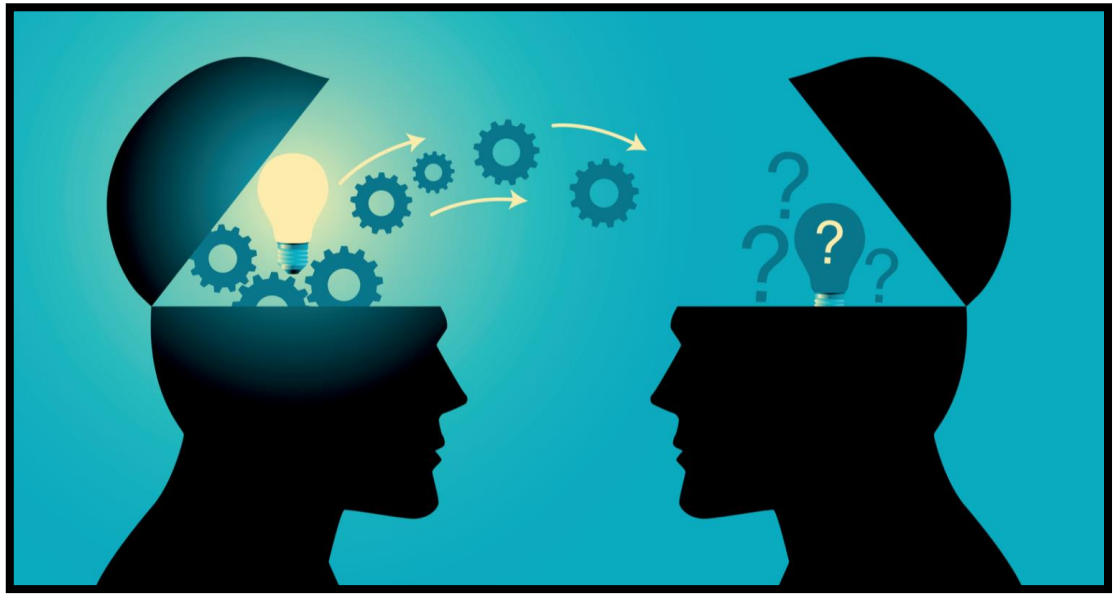
- Organizational changes
- Information systems (new/changes)
- New vendors
- Policies (new/revisions)
- New markets

Governance and Strategic Planning for Security

Information Security Governance – National Association of Corporate Directors Cyber Principles

Guidance from the NACD on how to handle risk as it relates to the cyber domain:

1. Understand and Approach Cybersecurity as an Enterprise Wide Issue, Not Just an IT Issue
2. Understand the Legal Implications of Cyber Risks as They Relate to the Company's Specific Circumstances
3. Have Adequate Access to Cybersecurity Expertise and Give Cyber Risk Management Regular and Adequate Time on Board Meeting Agendas
4. Set the Expectation That Management Will Establish an Enterprise-wide Risk Management Framework With Adequate Staffing and Budget; Specifically recommends NIST CSF
5. Management Discussions Should Include Identification of Which Risks to Avoid, Which to Accept and Which to Mitigate or Transfer Through Insurance



Governance and Strategic Planning for Security

Information Security (InfoSec) Governance Objectives and Desired Outcomes

What are you hoping to achieve via information security governance and how will you achieve it?

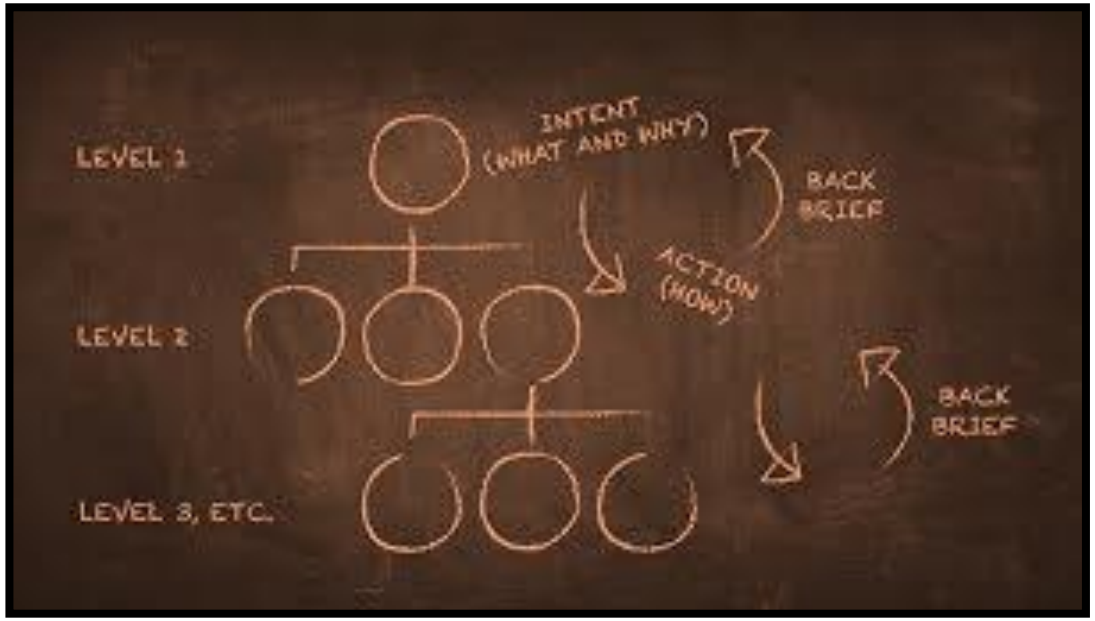
- **Several models are available for use**
- **The key to success is selecting the right model and applying it**
  - A governance program should be tailored to size and structure of the organization
- **Simple is often better**
  - Better to start simple and mature over time; ensures highest levels of ROI are maintained
- **Desired outcomes**
  - Strategic alignment of IS with business strategy
  - Risk management by executing appropriate measures
  - Efficient resource management
  - Performance measure to assess effectiveness

Governance and Strategic Planning for Security

Planning for Information Security (InfoSec) Implementation (I)

How do we create the InfoSec program?

- **Planning team must be cross-functional**
- **InfoSec projects must be properly planned beginning with investigation:**
  - What is the scope?
  - Who is impacted and how?
  - What are the priorities?
- **Investigation should be methodical and not a knee jerk reaction to a breach**
- **Questions to be answered:**
  - What are the core objectives? (For example, addressing newly discovered vulnerability(s); securing a new system; integrating a recently acquired company, etc.)
  - Are there legal requirements or guidelines?
  - What are we trying to accomplish?
  - What resources do we need?

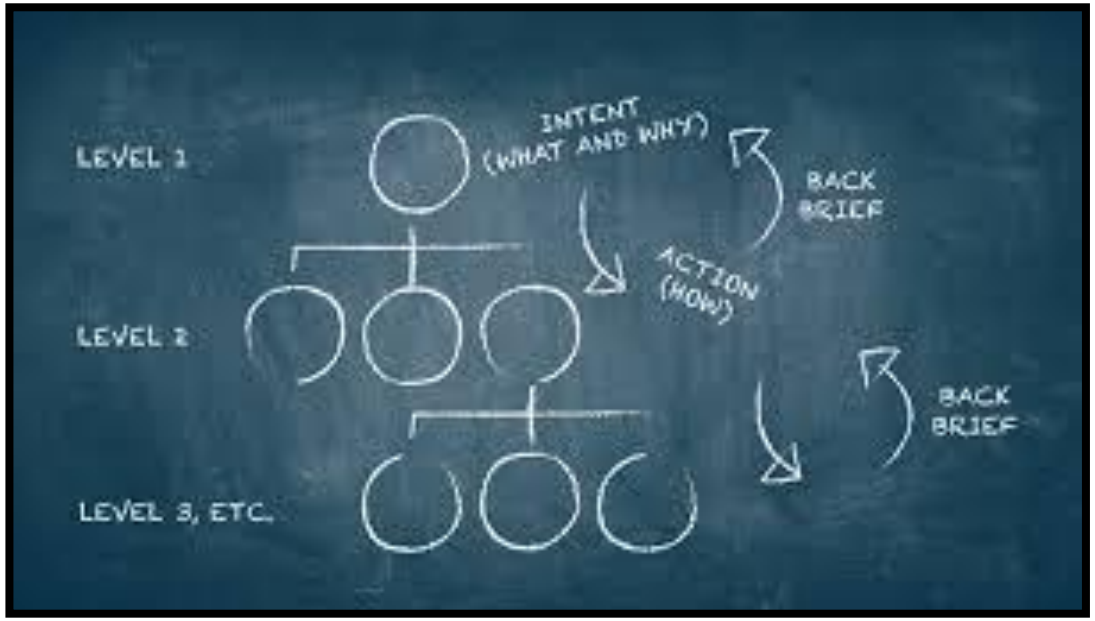


Governance and Strategic Planning for Security

Planning for Information Security (InfoSec) Implementation (II)

How do we create the InfoSec program? (continuation)

- **Context and priority will drive urgency**
- **Tailor the design to specific threats and risks**
- **Formulation phase for controls and safeguards**
- **Cross functional teams may need to be expanded (to advantage a range of IT expertise)**
- **Categories of controls:**
  - Managerial (ex. security planning process)
  - Operational (ex. incident response)
  - Technical (ex. access controls, monitoring)
- ***Information security plan* ties it all together**



Governance and Strategic Planning for Security

Planning for Information Security (InfoSec) Implementation (III)

How do we implement the InfoSec program?

- **Traditional project management methodologies apply**
- **Spend the appropriate amount of time planning**
- **Good planning makes implementation easy**
- **Start with easier projects to gain buy-in and momentum**
- **New threats are constantly emerging so your InfoSec program and plan needs to be adaptable quickly**
- **Maintenance activities include:**
  - External and internal monitoring (ongoing)
  - Risk assessments (annually)
  - Vulnerability assessments and remediation (quarterly)
  - Penetration testing (annually)

Module #3

Developing the Security Plan

Developing the Security Plan

Organizing for Security

Information security (InfoSec) program : The entire set of activities, resources, personnel, and technologies used by an organization to manage the risks of its information assets.

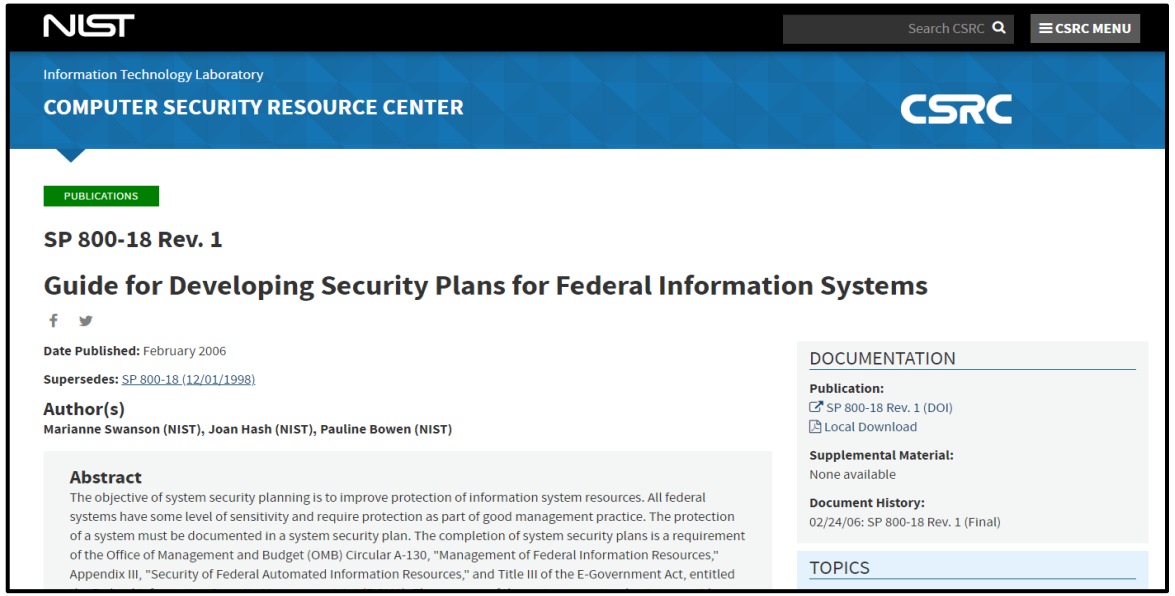
- **Structure variables:**
  - Industry
  - Culture
  - Size
  - Security staff and capital budget
- **An organization's size and available resources directly affect size and structure of an InfoSec program**
- **Most security programs are severely under-resourced and lack widespread support**
- **The larger the organization, the more disproportional information security programs seem to be**

Developing the Security Plan

Solid Examples of Frameworks Used in the Development of an Information Security (InfoSec) Program Plan

Leverage NIST publications

- SP 800-18 Rev. 1



https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

Although it was written for those wishing to draft plans in defense of US Federal Information Systems, many have used it as a benchmark document from which to formulate their own enterprise's InfoSec plans, especially if wanting to do business with the US Government!

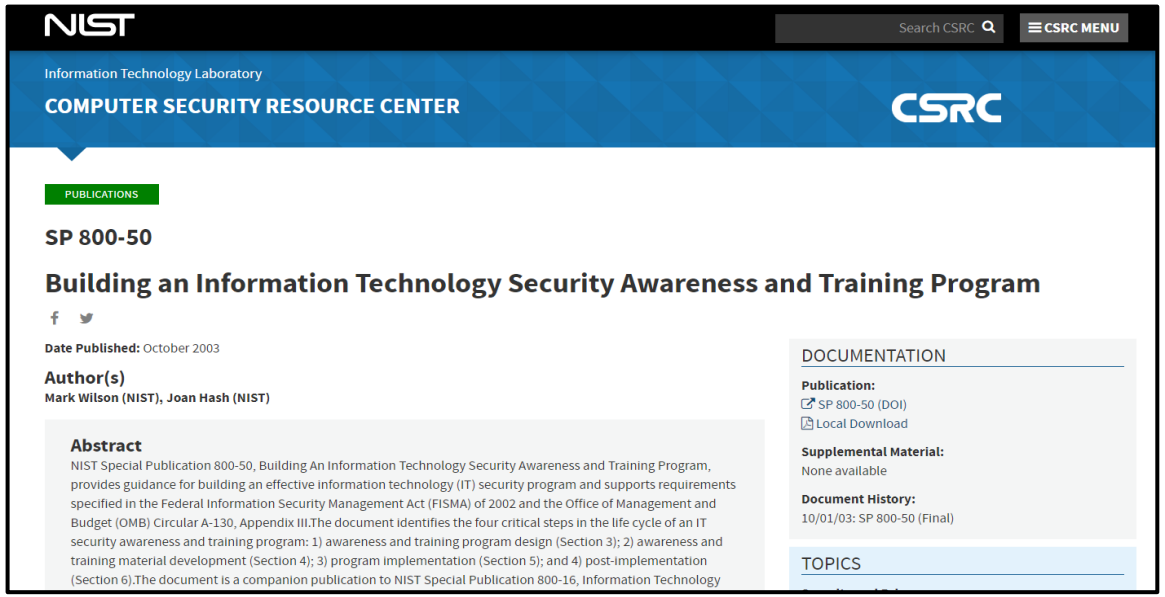
Developing the Security Plan

Solid Examples of Frameworks Used in the Development of an Information Security (InfoSec) Program Plan

Leverage NIST publications

- SP 800-12 Rev. 1 and SP 800-50

https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final



https://csrc.nist.gov/publications/detail/sp/800-50/final

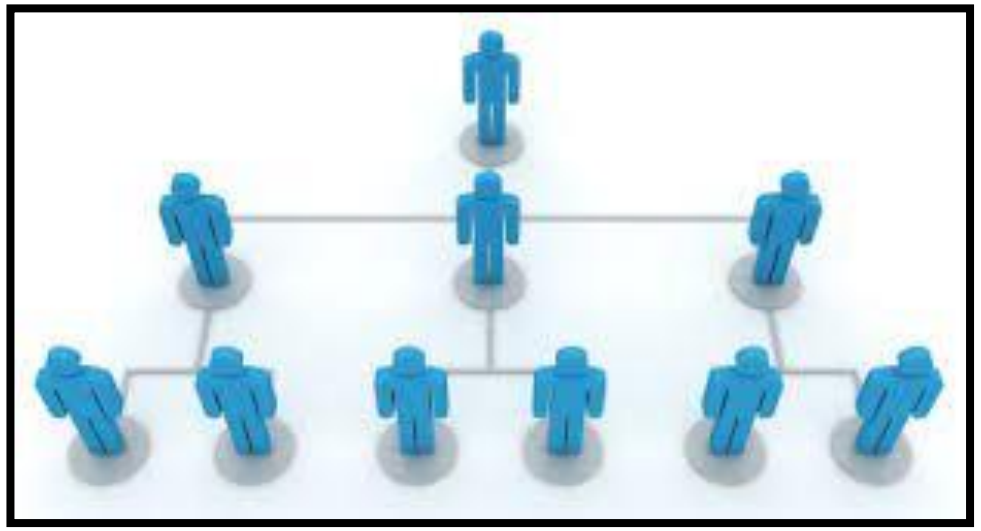
These seminal documents which provide guidance on InfoSec-related policy drafting may also help those responsible for writing broader plans, particularly if geared towards certain aspects of security or operations (i.e., training, etc.)!

Developing the Security Plan

Placing Information Security (InfoSec) Within an Organization

Chains of responsibility and reporting chains:

- **Information security ideally should not fall under IT organization**
  - "The people who do and the people who watch shouldn't report to a common manager"
  - Conflicts of interest arise when the people who are responsible for securing IT assets are the same ones who get to tell the boss whether something has happened
- **CISO's organizational reporting options:**
  - CISO reports directly report to CEO/President
  - A department (with no conflict of interest) inherits reporting duties
  - Reporting duties are an additional duty for (another) existing manager



Developing the Security Plan

Operational Components Addressed in the Development of an Information Security (InfoSec) Program and Plan

Security Program and Plan Components:

- Policy
- Program management
- Risk management
- Life-cycle planning
- Personnel/user issues
- Preparing for contingencies and disasters
- Computer security incident handling
- Awareness and training
- Security considerations in computer support and operations
- Physical and environmental security
- Identification and authentication
- Logical access control
- Audit trails
- Cryptography

*Note: The list above is by no means exhaustive. The management of each enterprise crafting a security program must do so based on the individual situation and resources available to that enterprise in a manner which suits that organization's charter and satisfies the customer base.

Developing the Security Plan

Security Program Success: Key Considerations

Program and plan success (key considerations):

- Program/plan needs to be tailored to the organization
- Most components (shown on the previous slide) will be the same but size, products/services, regulatory environment and funding will drive program
- Executive team's support of the program will ultimately determine its drive, structure, and effectiveness

Module #3

Developing Security Program Components:

Implementing Security Education, Training, and Awareness (SETA) Programs

Developing the Security Plan

Implementing Security Education, Training, and Awareness (SETA) Programs (I)

SETA (Program): A managerial program designed to improve the security of information assets by providing targeted knowledge, skills and guidance for employees.

- **Education** – seeks to educate organization on why it has prepared the way that it has
- **Training** – seeks to train members on how to react and respond to specific threats
- **Awareness** – seeks to teach what security is and what to do in certain situations

Developing the Security Plan

Implementing Security Education, Training, and Awareness (SETA) Programs (II)

- **SETA Purpose**
  - Building in-depth technical knowledge
  - Developing end-user skills and knowledge to securely safeguard information assets
  - Improving and raising awareness

- **SETA Benefits:**
  - Improve(s) employee behavior
  - Inform(s) employees about reporting violations
  - Enable(s) organizations to hold employees accountable for actions

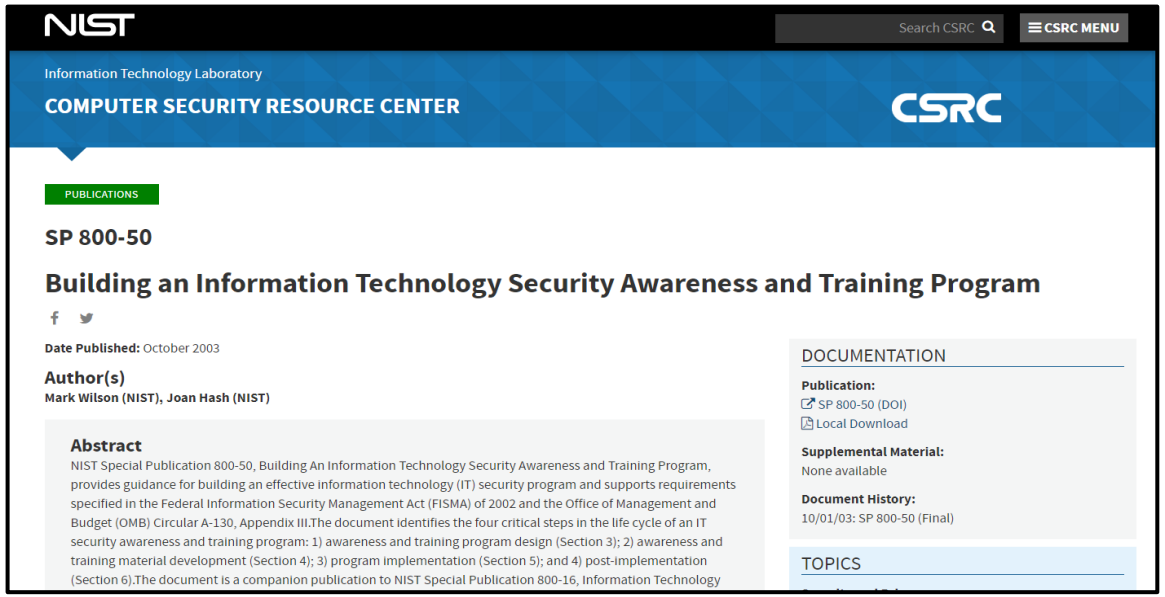
Developing the Security Plan

Solid Examples of Frameworks Used in the Development of an Information Security (and SETA) Program

Leverage NIST publications

- SP 800-12 and SP 800-50

https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final



https://csrc.nist.gov/publications/detail/sp/800-50/final

Developing the Security Plan

Employee Training Awareness Collateral

What can an enterprise use to market optimal cybersecurity and information security to its personnel?

- Videos and podcasts
- Posters and banners
- Presentations and conferences
- Computer-based training
- Newsletters, brochures and flyers
- Trinkets (coffee cups, pens, etc.)
- Bulletin boards

For an abundance of free resources one can use to inform and educate others in cybersecurity and information security, please go to the following URLs:
https://www.us-cert.gov/publications/distributable-materials
https://www.cyberreadinessinstitute.org/

JOHNS HOPKINS
CAREY BUSINESS SCHOOL

Introduction to Cybersecurity

Module #4

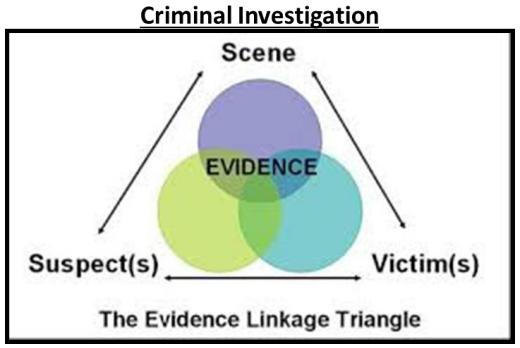
Cyber Threat Intelligence (CTF) and the Cyber Diamond Model (CDM) • The Mod #4 Chart Exercise • Issues Affecting Cyber Threat Intelligence Provision • Risk Management: Identifying, Assessing, and Controlling Risk • Identifying and Assessing Threats to InfoSec • The NIST Cybersecurity Framework (CSF) • Threat and Vulnerability Mapping • Identifying and Assessing Vulnerabilities to InfoSec • Combatting the Insider Threat

Module #4

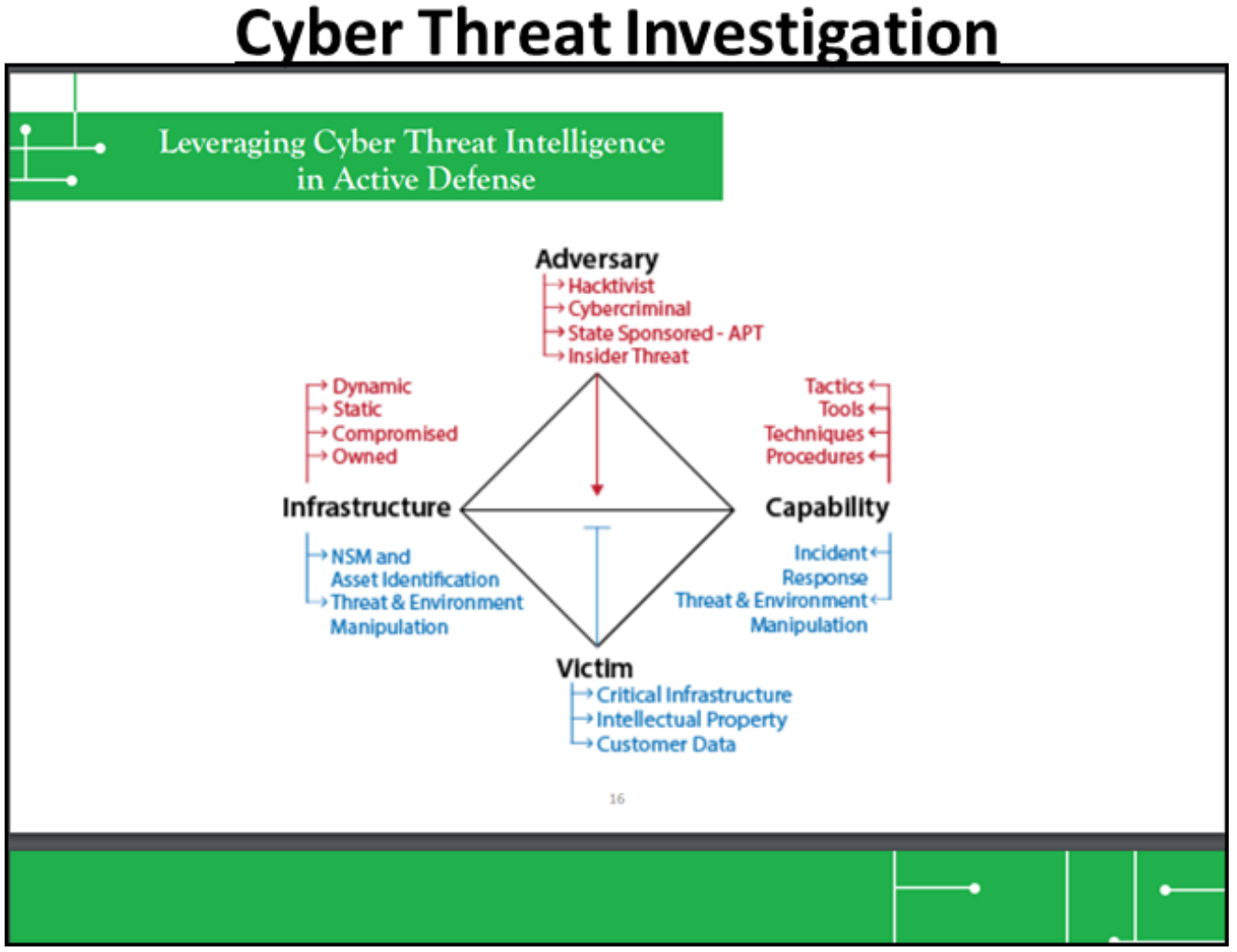
Cyber Threat Intelligence and the Cyber Diamond Model (CDM)

Cyber Threat Intelligence and the Cyber Diamond Model (CDM)

The Network Compromise as the Scene of a Crime: Using the Cyber Diamond Model (CDM)

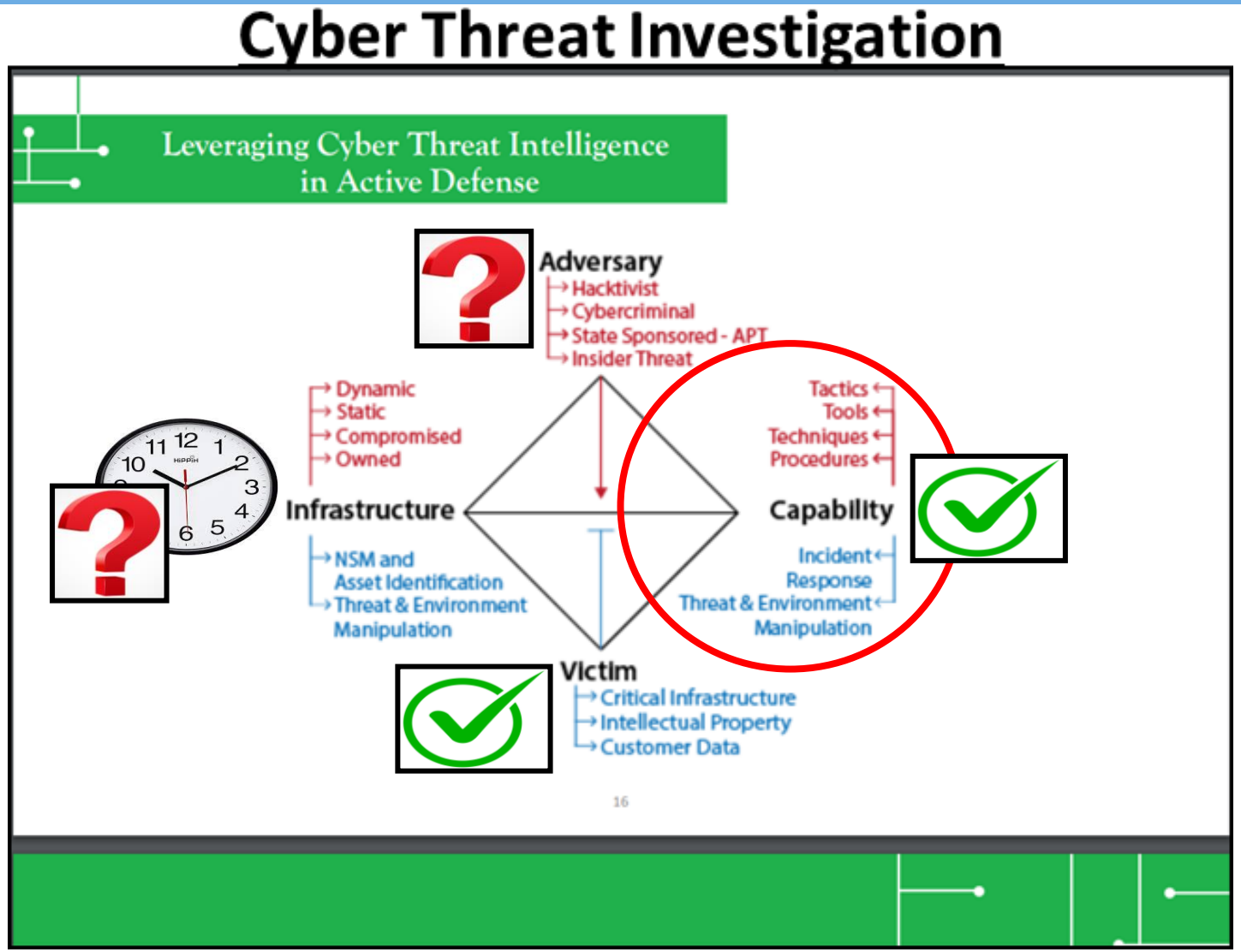


The conceptual criminal investigation model (shown above) is used by criminal investigators to determine and address the information gaps which exist after a violent episode occurs which they must later "piece together." The interaction between the three main elements – scene, suspect, and victim – provide a conceptual framework for collecting and analyzing evidence systematically. **The Cyber Diamond Model (CDM)** (right) is a conceptual framework used to address events in the cyber domain to reach similar ends in the systematic processing of evidence. "Victim" is a shared term, with "adversary" replacing the term "suspect," "infrastructure" loosely replacing "scene," and "capability" representing the tactic used to execute the compromise (akin to a *modus operandi, or MO*).



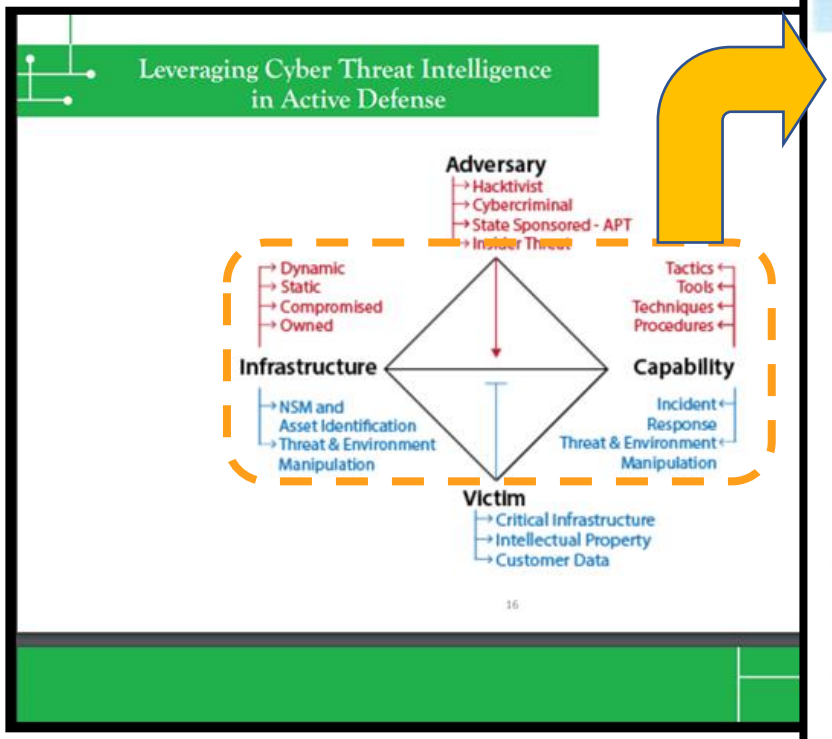
Cyber Threat Intelligence and the Cyber Diamond Model (CDM)

Particulars of the Cyber Diamond Model (CDM): Capability (II)



Cyber Threat Intelligence, the CTF, and the CDM

Using the Cyber Threat Framework (CTF) to Categorize Observed Activity for the Cyber Diamond Model (CDM)



(U) Cyber Threat Framework: Observable Malicious Activities

LAYER 1 - STAGES				
PREPARATION	ENGAGEMENT	PRESENCE		EFFECT
Actions to prepare to conduct cyber activities	*Actions to gain unauthorized access*	*Actions to maintain unauthorized access*		*Outcomes of actions on targeted system*
LAYER 2 - STAGES				
Plan Activity	Deploy Capability	Establish Initial Control	Establish Persistence	Deny access
Research & Analysis	Interact with Target	Hide	Expand Presence	Alter System Behavior
Resource/Capability Development	Drive-by attacks	Refine Targeting		Extract data
Conduct Reconnaissance	Exploit Vulnerabilities			Destroy HW/SW/Data
Stage Capabilities	Deliver Payload			Enable Other Operations
Initiate Operations	Suspicious Network Activity			
LAYER 3 - STAGES				
Review Strategy	Deploy Electronically	Unauthorized access	Anti-intrusion Detection Measures	Disrupt/Degrade Links
Plan Mission	Physical Proximity	Automated Malware C2	Anti-forensic measures	Disrupt/Degrade Network
Issue Guidance	Credential Farming	Establish Communications	Monitor Administrators	DDoS
Gather Intelligence	Social Engineering	Network Mapping	Increase User Privileges	Install Ransomware
Identify Targets	SQL Injection	Software Packing	Lateral Movement	Create Botnet(s)
Develop Infrastructure	Masquerade	Masquerading	Identify Targets of Opportunity	Deface Websites
Physical Reconnaissance	Use of Exploit Kit	Obfuscate Payloads	Service Manipulation	Relocate/Store Data
Electronic Reconnaissance	Cross Site Scripting	Indicator Blocking	Registry Run Keys	Disclose Data
Stage Externally/Internally	Webmail Vulnerability	Scripting	BIOS Rootkit	Exfiltrate Data
Issue Operational Tasking	App Vulnerability	Disabling Security Tools	Master Boot Record	Establish C2 or Hop Point

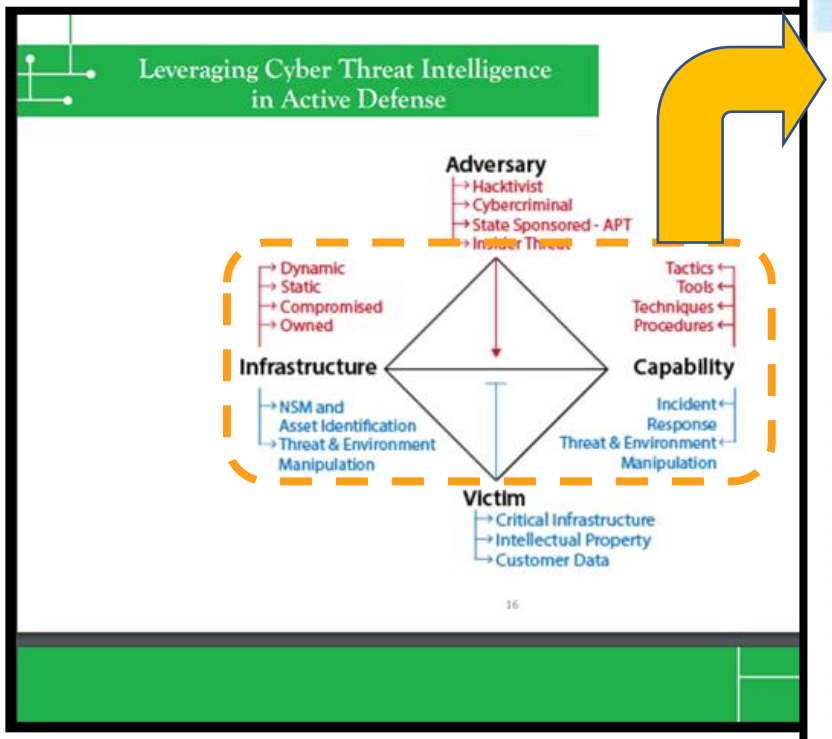
By taking Infrastructure- and Capability-related evidence collected in line with the Cyber Diamond Model and subjecting it to the Cyber Threat Framework, we can better assess to what extent the malicious cyber activity matches other observed activity from other events. This “matching” is what may potentially result in attribution, or identifying who the previously unknown adversary was who committed the hack so that action(s) may be taken against them, and defenses may be mounted against other tactics they are known to use.

Module #4

The Mod #4 Chart Exercise

Cyber Threat Intelligence

A Reminder of the Uses of the CDM and CTF before Jumping into the Mod #4 Chart Exercise



(U) Cyber Threat Framework: Observable Malicious Activities

LAYER 1 - STAGES				
PREPARATION	ENGAGEMENT	PRESENCE		EFFECT
Actions to prepare to conduct cyber activities	*Actions to gain unauthorized access*	*Actions to maintain unauthorized access*		*Outcomes of actions on targeted system*
LAYER 2 - STAGES				
Plan Activity	Deploy Capability	Establish Initial Control	Establish Persistence	Deny access
Research & Analysis	Interact with Target	Hide	Expand Presence	Alter System Behavior
Resource/Capability Development	Drive-by attacks	Refine Targeting		Extract data
Conduct Reconnaissance	Exploit Vulnerabilities			Destroy HW/SW/Data
Stage Capabilities	Deliver Payload			Enable Other Operations
Initiate Operations	Suspicious Network Activity			
LAYER 3 - STAGES				
Review Strategy	Deploy Electronically	Unauthorized access	Anti-intrusion Detection Measures	Disrupt/Degrade Links
Plan Mission	Physical Proximity	Automated Malware C2	Anti-forensic measures	Disrupt/Degrade Network
Issue Guidance	Credential Farming	Establish Communications	Monitor Administrators	DDoS
Gather Intelligence	Social Engineering	Network Mapping	Increase User Privileges	Install Ransomware
Identify Targets	SQL Injection	Software Packing	Lateral Movement	Create Botnet(s)
Develop Infrastructure	Masquerade	Masquerading	Identify Targets of Opportunity	Deface Websites
Physical Reconnaissance	Use of Exploit Kit	Obfuscate Payloads	Service Manipulation	Relocate/Store Data
Electronic Reconnaissance	Cross Site Scripting	Indicator Blocking	Registry Run Keys	Disclose Data
Stage Externally/Internally	Webmail Vulnerability	Scripting	BIOS Rootkit	Exfiltrate Data
Issue Operational Tasking	App Vulnerability	Disabling Security Tools	Master Boot Record	Establish C2 or Hop Point

By taking Infrastructure- and Capability-related evidence collected in line with the Cyber Diamond Model and subjecting it to the Cyber Threat Framework, we can better assess to what extent the malicious cyber activity matches other observed activity from other events. This “matching” is what may potentially result in attribution, or identifying who the previously unknown adversary was who committed the hack so that action(s) may be taken against them, and defenses may be mounted against other tactics they are known to use.

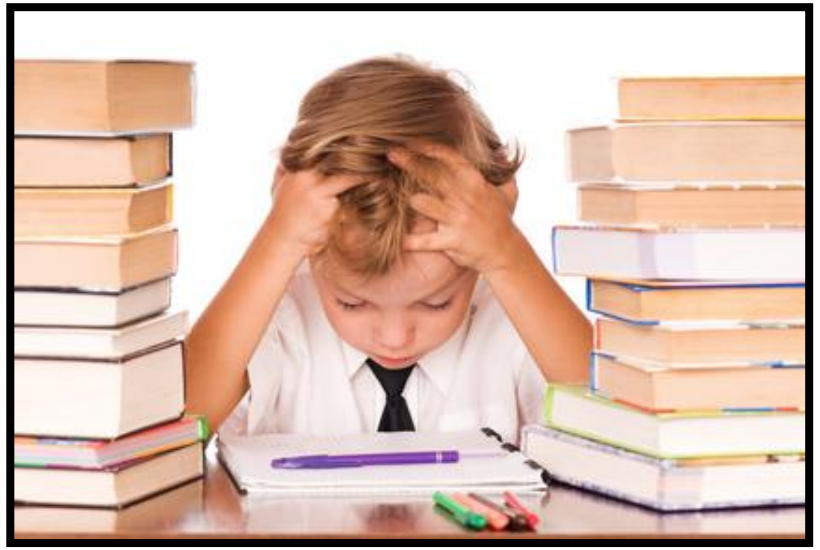
Module #4

Issues Affecting Cyber Threat Intelligence Provision

Issues Affecting Cyber Threat Intelligence Provision

Challenges to Leveraging the Info We Have or Obtaining the Info We Need to Heighten Cybersecurity

- **Enterprise data purging policies differ amongst stakeholders (with similar issues/equities)**
  - The overwhelming majority of enterprises with IT assets have a limit to the amount of data they can hold over time. They are forced to purge or overwrite data representing network activity which can never be retrieved.
- **Jurisdictions/stakeholders are rarely federated for effective cyber defense and information sharing**
  - Without robust information sharing, every enterprise and individual leaves themselves open to having to learn about a compromise by being the victim themselves.
- **Metrics are hardly ever revisited to ensure reliability to gauge continued accuracy in a dynamic environment**
  - Once a defensive measure is introduced to the world, the clock begins as to how long until that particular measure is circumvented. The data needed to establish such metrics is notoriously difficult to collect.



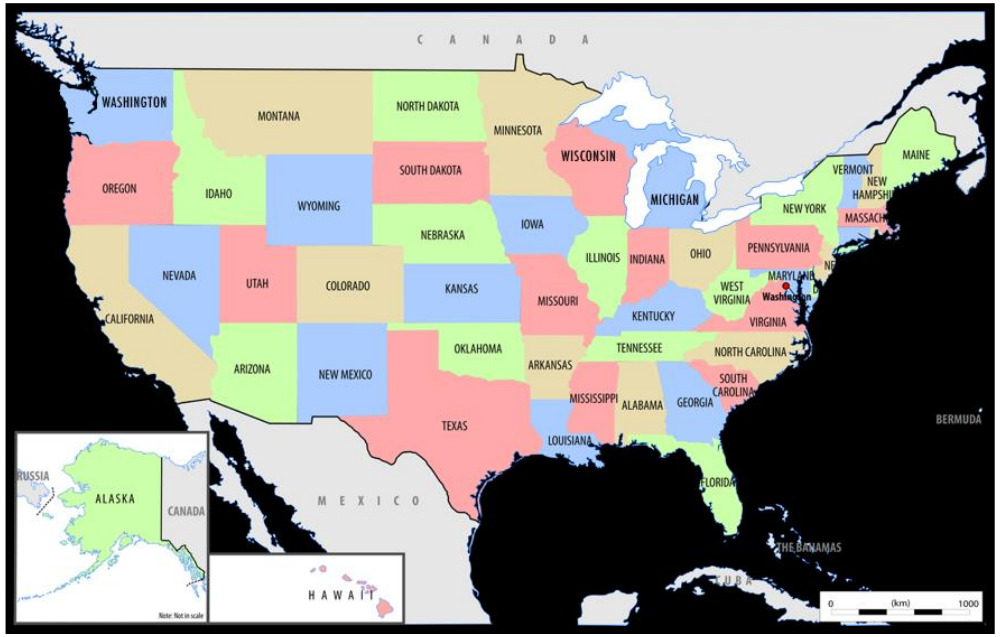
Issues Affecting Cyber Threat Intelligence Provision

Data Purging Policies

Who can cook with missing ingredients?

- The weakness lies in the fact that too many data gaps exist which make even a suitable sample size of cyber activity – over any extended period of time - difficult to amass. This situation, in turn makes it close to impossible to interpolate or extrapolate findings to in-group members or a broader population, respectively, with any confidence in accuracy.

**Remember: When it comes to the data used to make findings that will acted on, use the very best data available or else you will find yourself wondering why the findings do not reflect reality!!!*
(Garbage in, garbage out!)



In all, the 50 states and territories are comprised of 3,141 counties and equivalents; adding the District of Columbia gives **3,142**.

Question: How does one help this many network owners and operators to find commonality in cyber adversaries faced if they ALL purge the inputs, that you needed in order to help them, at different times with no possibility of retrieval?

Issues Affecting Cyber Threat Intelligence Provision

Non-Integrated Stakeholders

The greatest contribution most [enterprises] may make is to act as a warning to others. - Unknown

(This would be nice, if it were true. – Your Instructor)

- By one stakeholder not sharing information on what has occurred to their network – typically out of fear of reputational damage – every single other entity within that sector or competitive space with similar characteristics may now have to experience the very same disruption or destruction themselves.
- Groups such as **information sharing analysis centers (ISACs)**, for instance, in the United States, attempt to form coalitions amongst competitors or members in a field (e.g., scientific, commercial, utility-focused, financial, etc.) so that information can be shared freely between them and the government to everyone's benefit. This also precludes any one entity gaining a competitive advantage over all others due to having information first.

Issues Affecting Cyber Threat Intelligence Provision

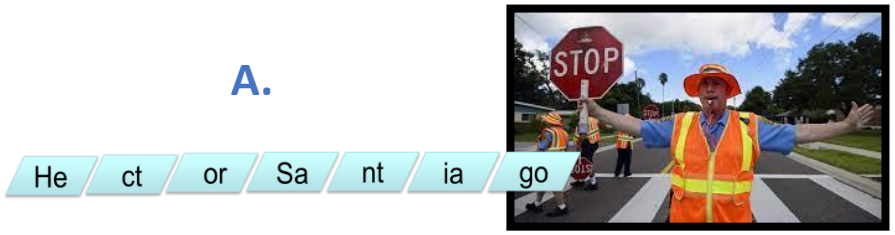
Use of Outdated/Outmoded Metrics

When was the last time you went for a check-up?

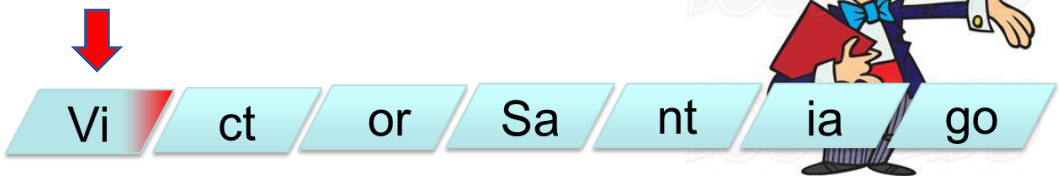
- **Diagnostics measuring the accuracy of metrics used for cybersecurity purposes are not being done with the frequency needed to ensure accuracy.**
  - By not ensuring upkeep of those measures and measurements used to help alert affected personnel that something aberrant is occurring to their network's health, no expenditures or resources applied to InfoSec can truly be justified. In other words, the result is a **VERY LOW RETURN-ON-INVESTMENT (ROI)** with regard to any cybersecurity in place.

. . . and now, an explanation of the modular threat, and why signatures have a limited "shelf life" in intrusion detection and prevention systems (IDS/IPS).

A.



B.



Module #4

Risk Management: Identifying, Assessing, and Controlling Risk

Risk Management: Identifying & Assessing Risk

Introduction to Risk Management

Risk Management: Identifying & Assessing Risk

Introduction to Risk Management

The four main questions concerning risk in InfoSec are:

- **Where is the risk to my information assets (risk identification)**
  - Ex. O365, Oracle, Salesforce, on-site servers
- **How severe is the risk to my information assets? (risk assessment)**
  - Impact - high, medium, low
- **What levels of risk am I willing to accept? (risk appetite)**
- **What do I need to do to bring my current level of risk down to an acceptable level? (risk control)**

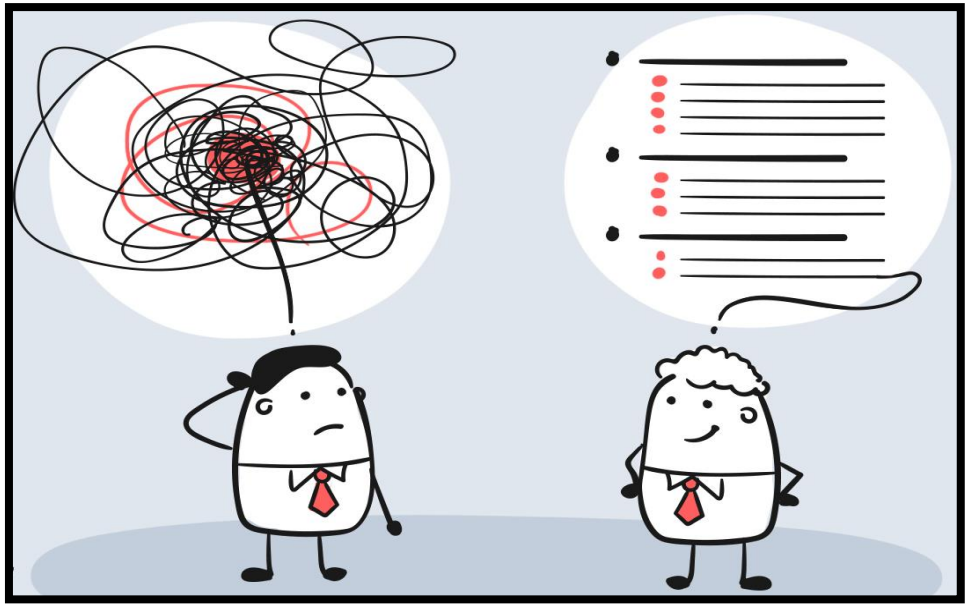
  Remember the 6 P's ? They are:
  - Plans
  - Policymaking
  - Protections
  - Programs
  - Personnel
  - Project Management

Risk Management: Identifying & Assessing Risk

Risk Identification

How do we identify risks amongst our information network assets?

- **Create an inventory of information assets**
  - Hardware, software, systems
- **Classify and organize those assets**
  - Public, private/confidential, regulated
- **Assign value to each asset**
- **Identify threats to cataloged assets**
  - External and internal
- **Identify vulnerable assets by tying specific threats to specific assets**
  - O365 SharePoint – stolen credentials, phishing, etc.

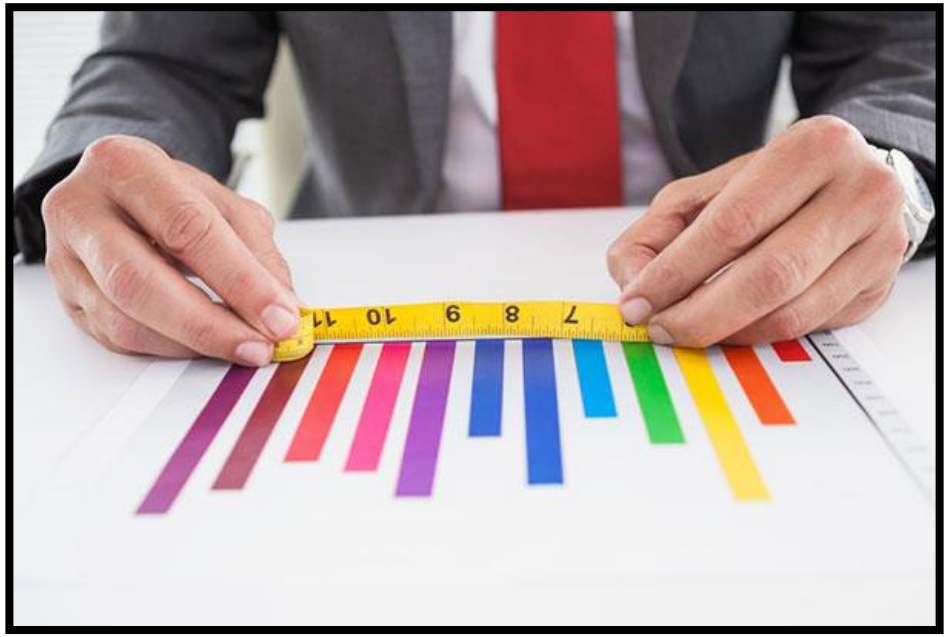


Risk Management: Identifying & Assessing Risk

Risk Assessment

How do we assess risks amongst our information network assets?

- **Determine likelihood that vulnerable systems will be attacked by specific threats**
  - e.g., espionage actors targeting competitors' networks used for R&D
- **Assess relative risk of organization's information assets (context and priority)**
- **Calculate the risks to exposed assets**
- **Assess controls that directly link to identified risks**
  - MFA, access controls, password complexity
- **Document and report findings**
  - Always leave a record of findings as systems/personnel will not be able to held for investigation in perpetuity



Risk Management: Identifying & Assessing Risk

Risk Appetite

What levels of risk do we accept for each of our information network assets?

- **Identify individual risk tolerances for each information asset**
  - Low priority assets have high risk tolerance
- **Combine individual risk tolerances into coherent risk appetite statements**

Risk Management: Controlling Risk

Risk Control Strategy

Risk control strategies typically fall into one of the following types:

- **Defense**
  - Firewall
  - Anti-virus software
- **Transference (sharing)**
  - Insurance
  - Cloud service provider
- **Mitigation**
  - Network segmentation
- **Acceptance**
  - Web site vulnerability
- **Termination**
  - Disable a known SharePoint application

***Note: The key to successful risk control evaluation is to consistently evaluate risks using same variables and process!**

- **Variables**
  - Impact
  - Likelihood
  - Control mitigation effect
  - Uncertainty

Risk Management: Controlling Risk

Risk Controls Evaluation

What types of controls do we put in place? Why? How?

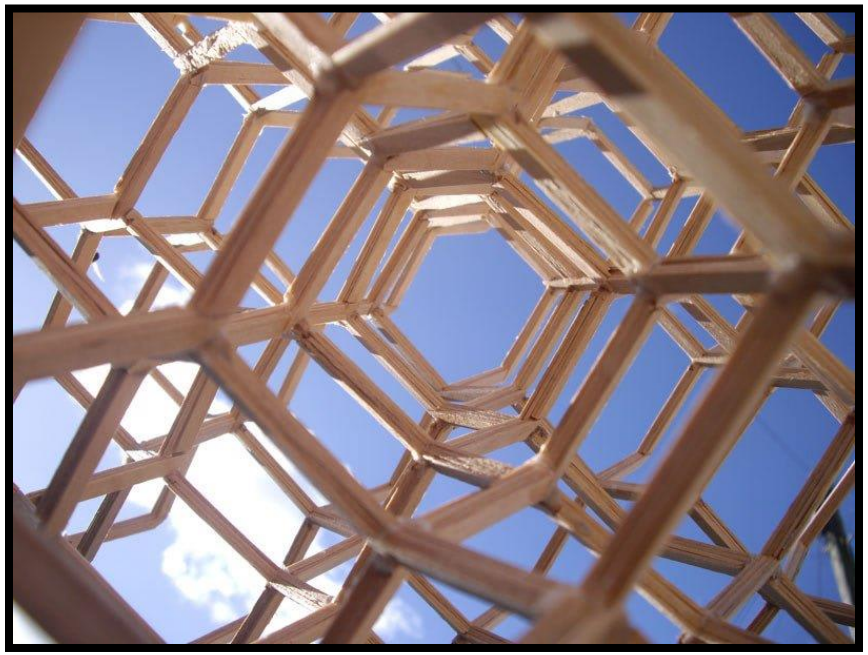
- **Determine which control options are cost effective and practical**
  - Approach will likely include mix of control options
- **Acquire and/or install appropriate controls**
- **Oversee processes to ensure controls remain effective**
  - Assessments, vulnerability scans, penetration testing, etc.

Risk Management: Controlling Risk

Risk Control Practices

Popular risk control models and frameworks include:

- **Delphi Technique**
  - Common approach for small/mid-sized firms
  - Primarily a qualitative approach
  - Good for initial assessment
- **OCTAVE Methods**
  - Original OCTAVE (larger organizations)
  - OCTAVE-S (smaller organizations)
  - OCTAVE-ALLEGRO
- **Microsoft Risk Management Approach**
- **Factor Analysis of Information Risk (FAIR)**
  - Focus is quantitative analysis
- **ISO 27005 Standard for InfoSec Risk Management**
- **NIST Risk Management Model**



Risk Management: Controlling Risk

Asset Valuation

How do we decide the worth of something we perceive to be an asset?

- Value Retained from Cost of Creating the Information Asset
- Value Retained from Past Maintenance of the Information Asset
- Value Implied by the Cost of Replacing the Information
- Value from Providing the Information
- Value Acquired from the Cost of Protecting the Information
- Value to Owners
- Value of Intellectual Property
- Value to Adversaries
- Loss of Productivity While Information Assets Are Unavailable
- Loss of Revenue While Information Assets Are Unavailable

Risk Management: Controlling Risk

Managing Risk – Key Terms

Expanding our risk management-related jargon; For example, how would we refer to risk metrics for an E-commerce web portal?

- **Annualized rate of occurrence**
  - Web portal unavailable 1x for 12 hours per year
- **Asset valuation**
  - Web portal supports $1M revenue per 24 hour period
- **Annualized loss expectancy**
  - Web portal unavailability costs $500k/year
- **Single loss expectancy**
  - $500k
- **Cost avoidance**
  - Redundant web server and access security control costs $50k/year
- **Cost-benefit analysis**
  - Security controls cost $50k/year
  - Spending $50k/year helps firm avoid $450k in projected lost revenue

Module #4

Identifying and Assessing Threats to InfoSec

The NIST Cybersecurity Framework (CSF)

Threat and Vulnerability Mapping

Identifying and Assessing Threats to InfoSec

Threat Identification

What (or who) do we perceive to be a credible actor which (or who) can act negatively against the information network assets of the enterprise?

- **Evaluation of threats to information assets and potential harm to organization**
  - Leverage industry specific intel groups, federal law enforcement, industry reports, etc.
- **One of the most important information security activities**
  - Creates a unique threat picture
  - Ensures most efficient deployment of resources

Identifying and Assessing Threats to InfoSec

Threat Assessment

How do we characterize threats so that we may then prioritize where to allocate resources?

- **Which threats represent actual danger to our information assets?**
- **Which threats are internal and which are external?**
- **Which threats have highest probability of success?**
- **Which threats could result in greatest loss if successful?**
- **Which threats is organization least prepared to handle?**
- **Which threats cost the most to protect against?**
- **Which threats cost the most to recover from?**

Identifying and Assessing Threats to InfoSec

Threat Examples

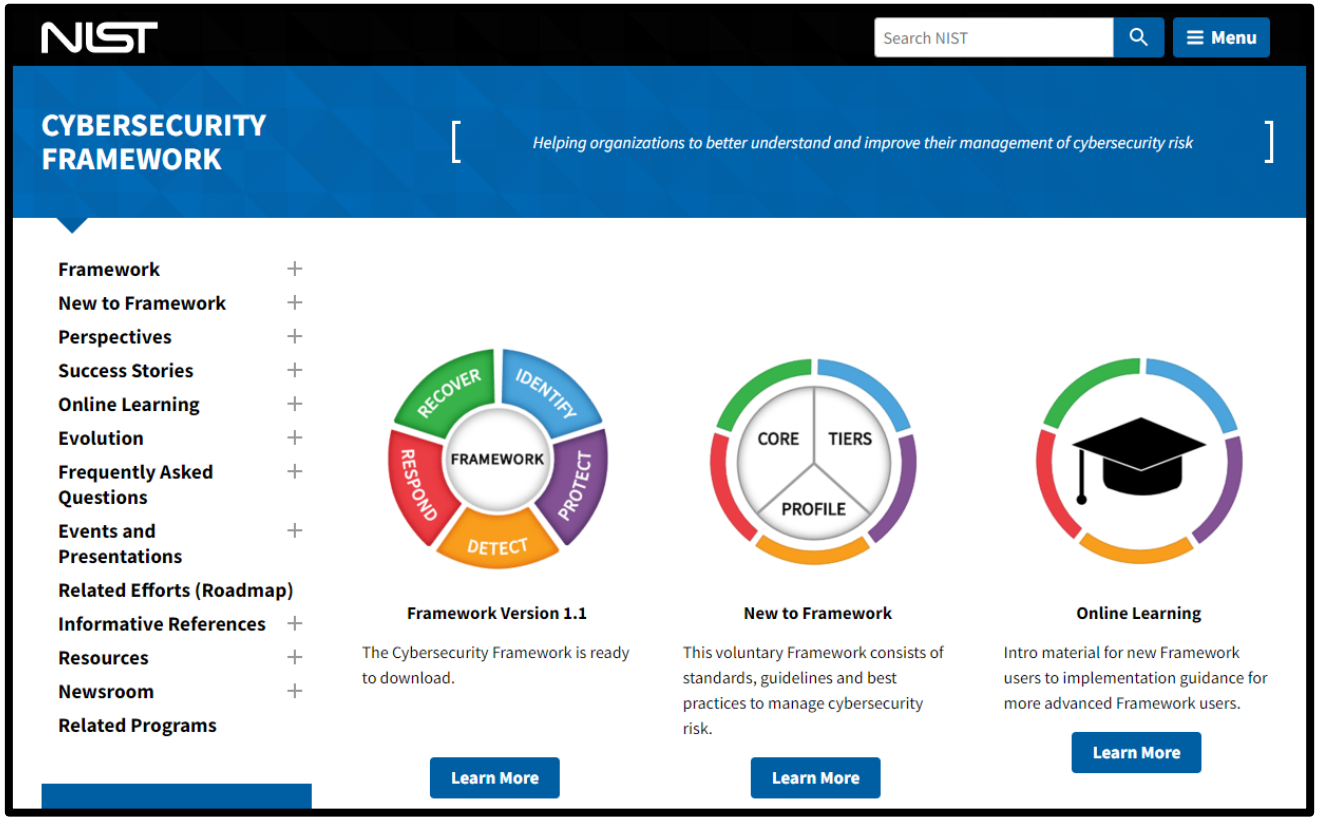
What are examples of the more common types of threats we can expect to challenge our InfoSec?

- Phishing/Spear Phishing
- Ransomware
- Malicious Insider Threat
- Negligent Insider
- Social Engineering
- Denial of Service
- Business Email Compromise

Threat and Vulnerability Mapping

A Popular Model for Identifying Internal Strengths and Gaps in Security: The NIST Cybersecurity Framework (CSF)

Leverage the NIST Cybersecurity Framework (CSF) to gauge the level of information network defense you are (and should be) deploying. Defensive components are broken up into five areas (shown in the graphic to the left).

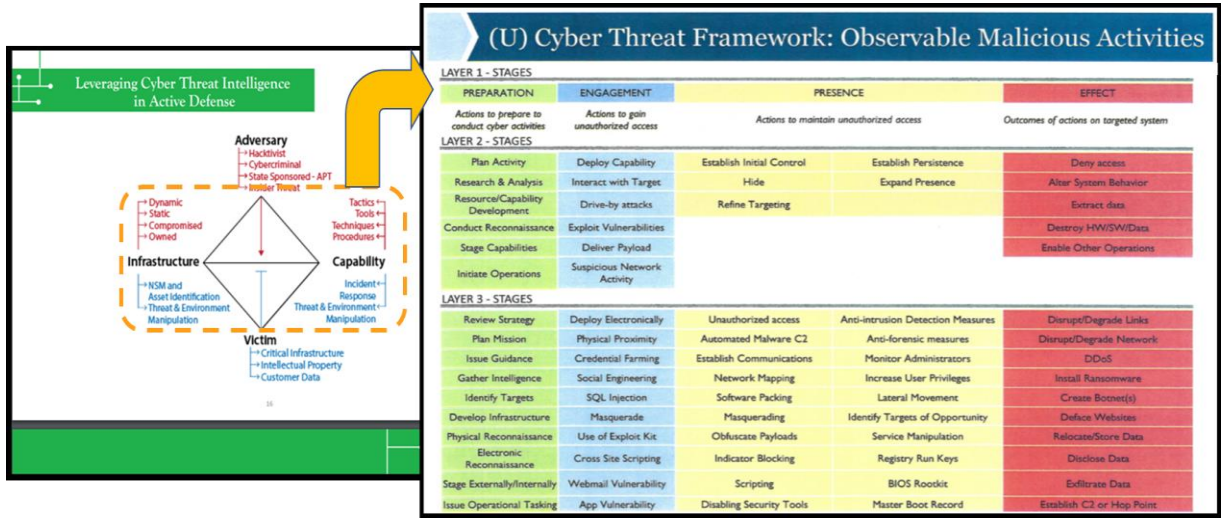


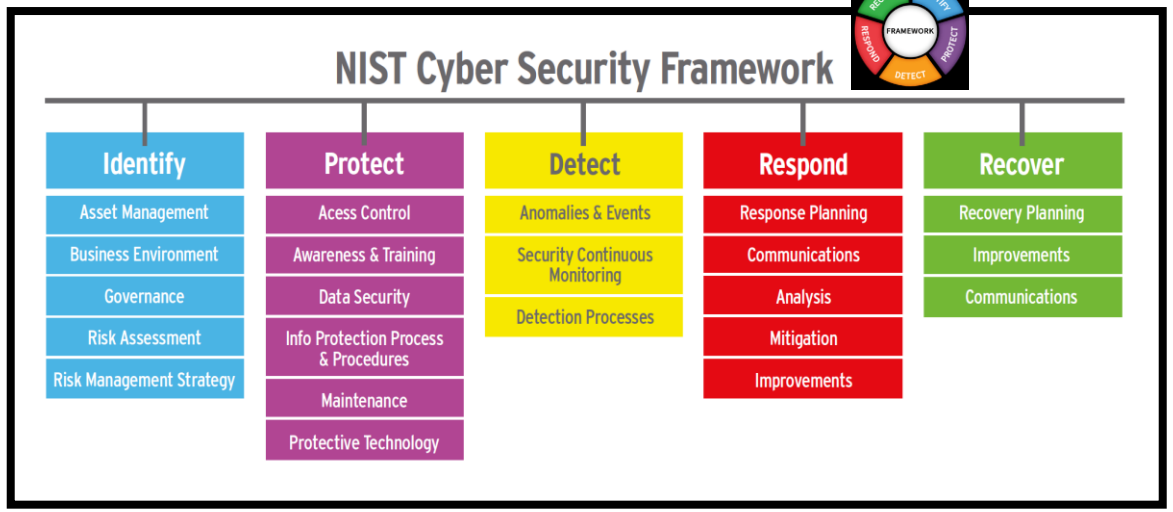
The CSF templates and guidance documents can be downloaded from the following URL: https://www.nist.gov/cyberframework

Threat and Vulnerability Mapping

How Popular Models and Frameworks are Used for Threat and Vulnerability Mapping

One example of what may be considered optimal threat and vulnerability mapping is the use of models such as the Cyber Diamond Model (CDM) and Cyberthreat Framework (CTF) (left) to collect and categorize observed adversarial cyber activity. Once the activities of the adversary are separated, each part of the adversarial tactic may be mapped to a particular aspect of the NIST Cybersecurity Framework (CSF) (right). When done correctly, findings will provide insights into the individual parts of your cybersecurity which need work!!!!





These models (above) are used to characterize <u>what the adversary is doing/did</u>.

This model (above) is used to characterize **what you/your enterprise is doing to defend your information network.**

By mapping what the adversary did to an aspect of security which should have alerted you/mitigated the threat, you may now begin to see EXACTLY where gaps exist for remediation and bolstering.

Module #4

Identifying and Assessing Vulnerabilities to InfoSec

Identifying and Assessing Vulnerabilities to InfoSec

Vulnerability Assessments and Relevant Considerations

Recommended actions when conducting a vulnerability assessment:

- **Drill down to specific avenues that threat agents can exploit to attack an information asset (i.e., triangulate root cause)**
  - Focus on flaws and/or weaknesses
  - People, policy and technology
- **A diverse group of assessors should be used**
  - Functional area expertise
  - Technical expertise
- **External assessors are recommended**
  - Required by some regulations and insurers

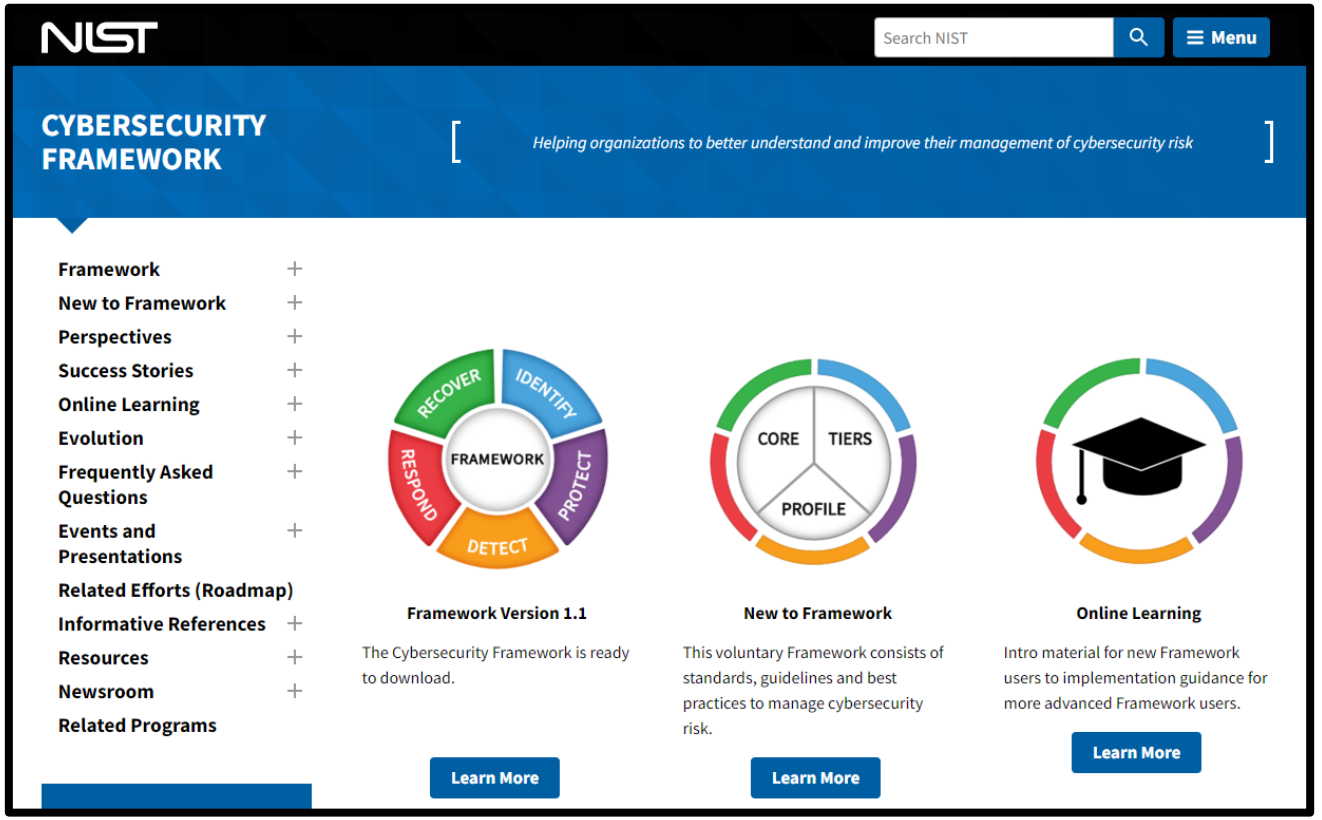
Considerations during the assessment and presentation of findings:

- **IT department will likely be initially defensive**
- **Assessment tools are becoming more expensive and specialized**
- **Assess all aspects of operations (i.e., people, policy and technology); Do not focus solely on technical vulnerabilities**

Threat and Vulnerability Mapping

A Popular Model for Identifying Internal Strengths and Gaps in Security: The NIST Cybersecurity Framework (CSF)

Leverage the NIST Cybersecurity Framework (CSF) to gauge the level of information network defense you are (and should be) deploying. Defensive components are broken up into five areas (shown in the graphic to the left).

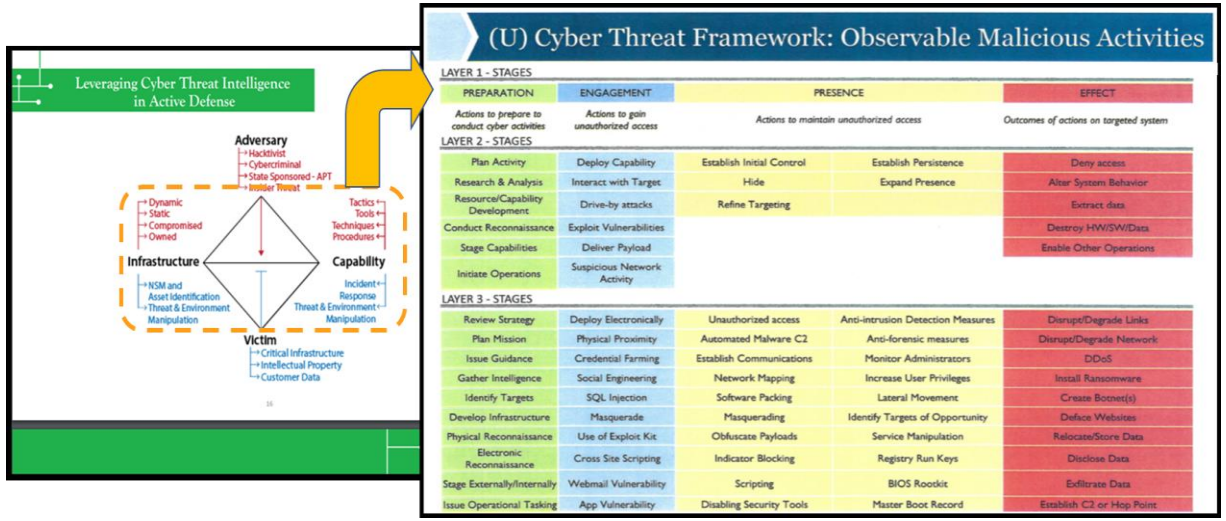


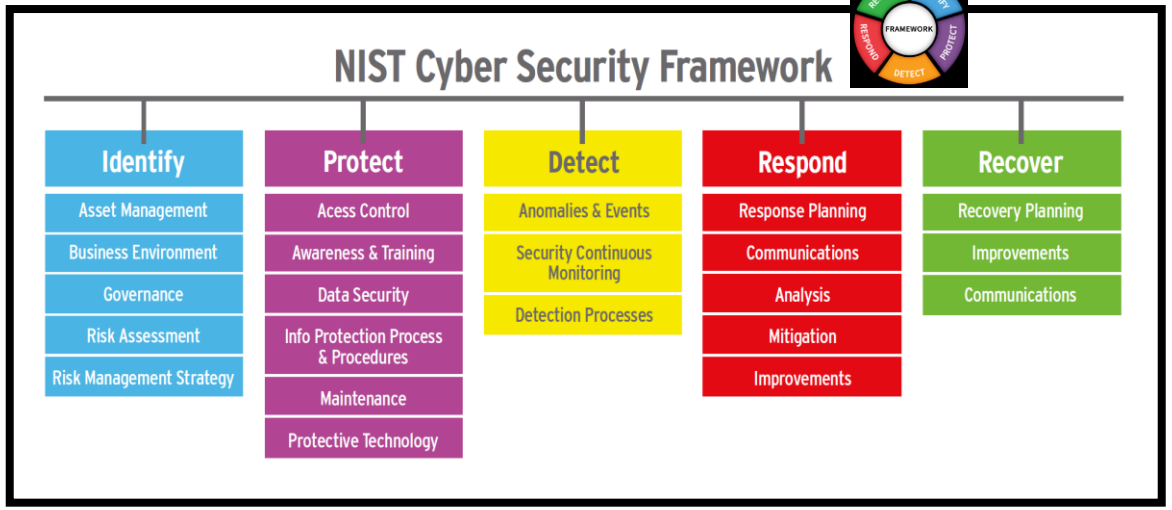
The CSF templates and guidance documents can be downloaded from the following URL: https://www.nist.gov/cyberframework

Threat and Vulnerability Mapping

How Popular Models and Frameworks are Used for Threat and Vulnerability Mapping

One example of what may be considered optimal threat and vulnerability mapping is the use of models such as the Cyber Diamond Model (CDM) and Cyberthreat Framework (CTF) (left) to collect and categorize observed adversarial cyber activity. Once the activities of the adversary are separated, each part of the adversarial tactic may be mapped to a particular aspect of the NIST Cybersecurity Framework (CSF) (right). When done correctly, findings will provide insights into the individual parts of your cybersecurity which need work!!!!





These models (above) are used to characterize <u>what the adversary is doing/did</u>.

This model (above) is used to characterize **what you/your enterprise is doing to defend your information network.**

By mapping what the adversary did to an aspect of security which should have alerted you/mitigated the threat, you may now begin to see EXACTLY where gaps exist for remediation and bolstering.

Module #4

Combatting the Insider Threat

Combatting the Insider Threat

Common Indicators of an Insider Threat (Specific to Cyber)

Common Indicators of an Insider Threat

Digital Warning Signs

- Downloading or accessing substantial amounts of data
- Accessing sensitive data not associated with their job function
- Accessing data that is outside of their unique behavioral profile
- Multiple requests for access to resources not associated with their job function
- Using unauthorized storage devices (e.g., USB drives or floppy disks)
- Network crawling and searches for sensitive data
- Data hoarding, copying files from sensitive folders
- Emailing sensitive data outside the organization

Combatting the Insider Threat

Common Indicators of an Insider Threat (Specific to Cyber)

Common Indicators of an Insider Threat

Behavioral Warning Signs

- Attempts to bypass security
- Frequently in the office during off-hours
- Displays disgruntled behavior toward co-workers
- Violation of corporate policies
- Discussions of resigning or new opportunities

Build for what's next™