Sylint®

# Cyber Security for Executives

## Critical Areas of Understanding

# 25 Cyber Security Questions

1 What is Cyber Security?

2 Why is Cyber Security relevant to us? Our organization’s information is public anyway.

3 Is Cyber Security an Information Technology problem or an Enterprise Risk?

4 Who is behind cyber attacks and data breaches?

5 What motivates malicious actors to conduct cyber attacks?

6 What is attribution and why is it difficult?

7 We have strong network perimeter defenses. Isn’t this enough?

8 Why are there so many security vulnerabilities in software, operating systems and applications?

9 If “patches” can fix software, operating systems and applications vulnerabilities, why are malicious actors still successful in exploiting information and operating systems?

10 What is the probability of an organization getting breached?

11 Is it possible to secure an entire network?

12 What should my security priorities be?

13 What considerations should be given to critical assets and information?

14 How can information be impacted by a Cyber Security event?

15 Which information security category typically has the highest impact potential?

16 How can malicious actors penetrate an organization’s network and operate undetected?

# 25 Cyber Security Questions

17 What is IAM and why is it so important?

18 Why are passwords not always effective?

19 What is multifactor authentication (MFA)?

20 What is encryption?

21 What is meant by “data-at-rest” or “data-in-transit”?

22 Why aren't AI and Behavioral Analytics sufficient?

23 Why should non-IT executives be aware of Cyber Security measures?

24 Why would non-IT executives be part of a Cyber Security incident response?

25 What are the potential repercussions of a data breach?

# What is Cyber Security?

Conceptually, Cyber Security encompasses, “measures taken to protect a computer or network of computers against unauthorized access or attack.” In the physical world, this is the community gate guard, the locks on the doors and the exterior *and interior* walls in the house.

## Our organization’s information is public. Why is Cyber Security relevant to us?

Attackers are also looking to disrupt operations and charge money to restore systems (e.g., ransomware), steal resources (e.g., computer processor power) to mine crypto-currency, disguise attacks against other companies, or just spread their message. Also, most organizations are in possession of information regarding operations, employees, clients, contributors, students or business associates that may be of future value to others.

## Is Cyber Security an Information Technology problem or an Enterprise Risk?

Cyber Security is an Enterprise Risk. Much of the data is outside IT’s direct control, and business operations determine the ability to implement and maintain security controls. While the locksmith can put a better lock on a door, that doesn't mean the business will let them (or that they even know the door exists). Enterprise Risk covers items with a significant impact on operations and potentially impacts the overall survivability of the organization.

## Who is behind cyber attacks and breaches of information security?

Actors behind cyber attacks typically fit into one of four categories:

1. Nation States & Terrorist Organizations
2. Organized Crime and other Criminals
3. Hacktivists
4. Industrial Espionage

As time progresses, lines between the categories have begun to blur based on available tools, attacker sophistication and information sharing between groups. Once a tool is developed and released "into the wild" it is available for anyone to wield, and attackers frequently draw from the same "pool" of tools in conducting their attacks.

# What motivates malicious actors to conduct cyber attacks?

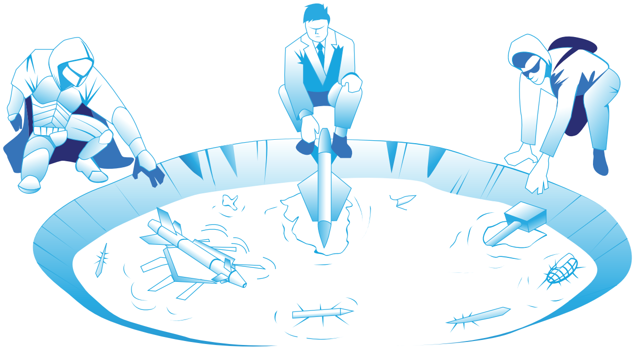
**Nation States** seek information to promote political, economic and military advantages. Their focus is typically strategic and they perform significant research on select targets. Their operations are usually long term in nature. Some Nation States have also begun using cyber attacks to self-finance their operations through activities normally seen in Industrial Espionage and Organized Criminal realms (e.g., ransomware, crypto-currency mining). Since they draw tools from the same 'pool' as everyone else, telling the difference between threat actors can be difficult.

**Terrorists** seek to promote uncertainty in the physical world and to enhance support of their stated objective or cause. Currently, terrorist organizations use cyber operations for command and control of their worldwide terrorist cells, to help fund and spread propaganda regarding their ideology, and to recruit membership into their terrorist organization. A terrorist may also covertly use third party cyber assets to obfuscate their location and operations.

**Organized Crime** groups seek financial benefits using the cyber domain as an additional means to support illegal operations and criminal activity while shielding their identity. Their focus is usually short term and potential victims include a wide range of targets that exhibit known Cyber Security vulnerabilities. They may use innocent third-parties to help shield their operations, and frequently use information from past victims to launch attacks against associated companies. These crime groups often operate as professional organizations with management and leadership structures and different business units charged with specific responsibilities (e.g., research, attack, reconnaissance, and monetization).

**Hacktivists** seek notoriety for social causes, such as their perception of animal rights or government inequities. Hacktivists typically target select entities with the objective of obtaining the maximum amount of publicity in hopes of generating additional support for their cause and to ruin the public perception and reputation of their target.

**Industrial Espionage** can take the form of small-scale insider threats or sophisticated operations with the backing of a Nation State. These actors work to shorten research & development cycles and increase profitability by stealing and leveraging someone else's work.



## What is attribution and why is it difficult?

Attribution is the act of relating a cyber attack to a particular group or individual. This is frequently based on comparisons of similarities in malicious code (malware), language, attack techniques, origin and other digital "fingerprints". However, these fingerprints are often masked by:

- Bouncing digital communications through commercial Virtual Private Network (VPN) companies or through a distributed network of relays operated by volunteers all around the world (i.e., TOR)
- Using otherwise innocent victims as launch points, and
- Using attack tools and techniques commonly associated with a different threat actor.

Nation States are particularly adept at using these techniques to maintain "plausible deniability" while conducting their operations. Organized Crime groups may be easier to identify, but use privacy laws, international regulations, and even their home-country's complicity to maintain operations. Ultimately, threat actors are drawing their tools and techniques from the same "pool" and it can be difficult to specifically identify who is behind the mask without a lot of cooperation and joint investigation.

## We have strong network perimeter defenses. Isn’t this enough?

Similar to early military defensive measures, initial stages of Cyber Security focused solely on perimeter defense. Employing a castle structure around the King’s residence provided some measure of protection; however, attackers eventually discovered methods to breach that perimeter (or waited until the King left) necessitating the concept of layered defenses. Just like interior doors & walls, locks & video cameras, and emergency generators & fire departments, secondary and tertiary cyber security controls provide additional opportunities for both detection and defense. Many times, *outbound* controls (e.g., web proxies & DNS protections) are as, or even more, important as *inbound* controls. Asking the question, "what happens if someone gets past that control" is an important part of understanding cyber security risks.

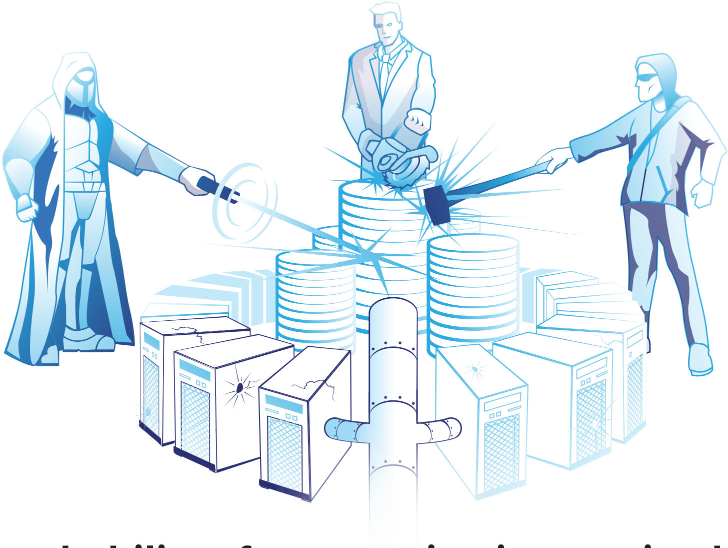
## Why are there so many security vulnerabilities in software, operating systems and applications?

Much like building a house, systems required to integrate with each other leave gaps through which attacks can occur. Software development is not a perfect process, and is generally measured around *operability* instead of *security*. A house without windows and doors is more secure, but not very functional. Single-source systems (e.g., Apple) tend to have fewer issues because of this tight integration between hardware and software.

## If “patches” can fix known software, operating systems and applications vulnerabilities, why are malicious actors still successful in exploiting information and operating systems?

Patching is hard. Complex network enterprises have interconnected systems that are fragile in nature. Even with automatic patch processes, updates have the potential to induce a corresponding system failure that dramatically impacts operations, and the business unit (*not* IT) may be unwilling to take that operational risk. Even where patching is possible, IT staff generally test patches in a nonproduction network prior to installing on operational systems to reduce the likelihood of patch-induced issues. All of these delay patch installation, and require alternative mitigation or protection strategies.

An additional challenge is that while hardware, operating systems and applications remain functional, support for the product may have been discontinued in the expectation of customers upgrading or refreshing equipment. Those unable to upgrade or on a long refresh cycle are on their own for vulnerability mitigation, and again need to find alternative protection.



## What is the probability of an organization getting breached?

Federal Bureau of Investigation (FBI), National Security Agency (NSA) and Securities and Exchange Commission (SEC), among others, have each stated numerous times that there are two types of organizations:

- **Those who know** they have experienced a Cyber Security breach
- **Those who do not know** they have been breached

Although that statement may not be entirely accurate, it defines the scope of the issue very well. Breaches at some level are unavoidable; much of the battle is *detection, response* and *containment*. These activities should be practiced in a "tabletop" or similar exercise to help prepare for the inevaitable.

## Is it possible to fully secure an entire network?

With omnipresent vulnerabilities within network systems, the addition of cloud computing and Internet of Things (IoT) devices, and attackers proficient in finding any gap to exploit, achieving complete network security is improbable. That doesn't mean the battle is lost, but does mean that a security program needs to be built around planning for failure. A grocery store will always have produce fall off shelves; the objective is to detect the fall, minimize the cascading effects, and quickly clean up the mess.

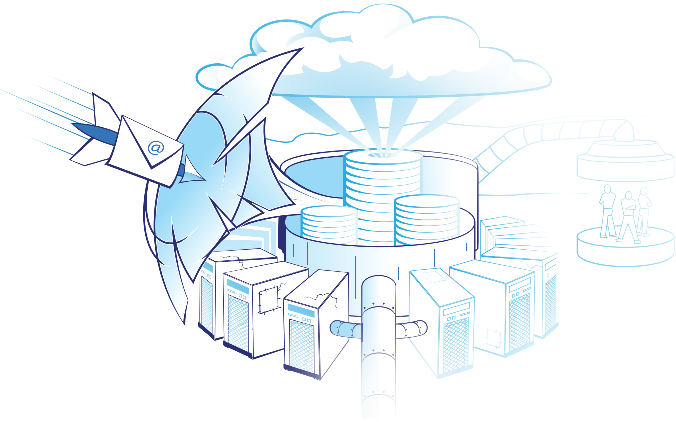
Users remain among the most difficult part of a network to secure. Security awareness and training can only accomplish so much as attackers routinely take advantage of user's job functions to introduce phishing messages (e.g., invoices from legitimate vendors, reservations or orders from likely customers) and conduct other social engineering attacks aimed at capturing credentials or installing malicious software (malware). Once threat actors have foothold, they can rapidly disappear into what appears to be legitimate user activity.

## If it is impossible to secure an entire network, what should be the priority?

Common attack vectors such as email and remote access can also have common mitigations (e.g., mail filters and multifactor authentication). At some point, not having these mitigations just invites attacks much like leaving a garage open or car running unattended. Internal gates and walls (segmentation) establish tripwires and smaller areas where increased security can be applied. Receiving, reviewing and acting on actionable threat intelligence can further help with a specific prioritization process. Maintaining up-to-date security tools and techniques, and measuring their implementation and usage, can minimize the impact of an incident.

Core objectives of an attacker should be considered when prioritizing security.

- Identify critical systems or sensitive information which, if compromised, could cause a significant negative impact to the organization
- Review routes and methods that attackers would need to take in order to compromise these systems
- Harden or secure those routes
- Identify key performance indicators to make sure that controls are, and remain, in place



## What considerations should be given to critical assets and information?

Critical assets and sensitive information can be secured and protected through a process that starts with *identifying* these particular assets and information and then determining their locations within the enterprise network. Once located, considerations can be made to:

- Consolidate data locations
- Destroy unnecessary or outdated data
- Minimize access (least privilege concept of operations)
- Monitor for compliance and abnormal activity

## How can information can be impacted by a Cyber Security event?

Impact to information is usually discussed in terms of "Confidentiality", "Integrity" and "Availability", or CIA.

**Confidentiality** refers to limiting access to information. Potential security measures to preserve data confidentiality include specifically granted credentials and information encryption in case it is lost or stolen. Additional security measures could include isolating computer systems, disconnecting storage devices or transitioning to "hard copy" (non-digital) data only. Data breaches are typically associated with the loss of information confidentiality. A loss of confidentiality can be difficult to detect unless the attacker announces their activity.

**Integrity** involves ensuring consistent, accurate and trustworthy data over the lifecycle of the information. The goal is to ensure data is not unintentionally changed. Security measures include cryptographic checksums (the outcome of running an algorithm on a piece of data for verification of integrity), integration into a blockchain, and maintaining multiple copies for comparison or recovery (e.g., backups). Cyber attacks impacting the integrity of data can be some of the most difficult to remediate since they can be executed at many levels and usually involve legitimate, though malicious, access to the data in question.

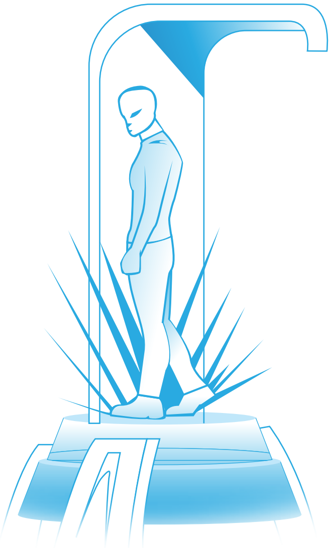
**Availability** is one of the easiest states to recognize and validate. It is associated with he functionality of systems that store, control or display information, or with the accessibility of the data itself.

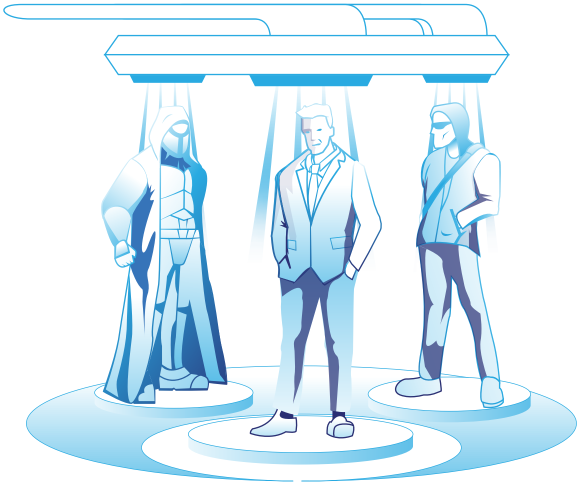
Furthermore, availability identifies with security measures to promote the assurance of functioning hardware and software operating systems, adequate bandwidth and redundancy. Disaster recovery measures are usually associated with maintaining or restoring the availability of information. Cyber attacks using encrypting malware (e.g., ransomware) to deny availability are popular with many types of attackers.

## Which information security category has the potential for the highest impact?

Unfortunately, each category has the potential for significant impact, and defenders have to be prepared for attacks against each area. Loss of Confidentiality can be invisible and devastating if the information involved is critical intellectual property or regulated data. Attacks against Integrity can be difficult to detect or recover from unless significant preparation is made in advance. Once the integrity of information is compromised, user and system trust are typically lost and rarely regained. Availability of information is basically a binary effect in that one either has or does not have access. If access is unavailable, then alternatives are necessary until operations can return to normal.

Conducting a cross-business unit Risk Analysis can help determine the relative impact(s) and path to recovery for each category. This doesn't have to be an expensive proposition, but instead requires a few hours of careful thought and consideration on potential attacks and their resultant impact and recovery requirements.





## How can malicious actors penetrate an organization's network and operate undetected?

Attackers are heavily incentivized, whether by power (nation state), fortune (organized crime) or fame (hacktivist), to successfully attack, move laterally and persist in a victim's network. Generally, the longer an attacker can operate undetected, the more successful they will be. Attacker workflow is frequently:

- Researching public-facing sites and systems, and identifying possible attack vectors (e.g., RDP, VPN and Mail servers)
- Leveraging missing patches, shared credentials, single-factor authentication and multi-use accounts that have been guessed, cracked, or acquired through other attacks to establish a foothold
- Once inside, using common system administrative tools to blend in with legitimate user or system activity
- Removing or degrading defense tools to avoid detection

## Why are passwords not always effective?

Stolen Passwords allow malicious actors to gain access to a device or network masquerading as an authorized user. Once an attacker gets one password, there are many ways to leverage this to gain additional access, including internal vulnerabilities, cached credentials, keystroke logging. Beyond social engineering, there are many ways those initial passwords are exposed:

- **Guessed:** “Password1”, "Spring...", "Fall..." and "Winter..." all meet standard complexity rules, and yet are easily guessed by attackers.
- **Reused:** Users frequently find one or two favorite passwords and use them across multiple sites; this allows the breach of one site (e.g., LinkedIn) to impact many other sites and services.
- **Stored:** Attackers can extract passwords that were used previously (cached credentials) and, if they haven’t been changed, reuse them in other areas.

Additionally attackers may also circumvent password requirements and access systems and data repositories directly through various exploits and vulnerabilities.

## What is multifactor authentication (MFA or sometimes 2FA)?

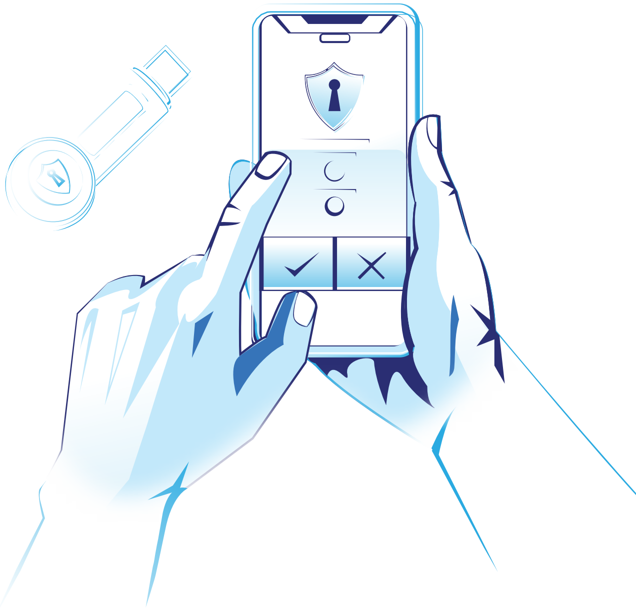
Simply put - something you *have* (e.g., a phone) and something you *know* (e.g., a password). MFA is a means of increasing the likelihood that the person requesting access is who they say they are, thus *authenticating* the user.

This one security measure can make a significant impact to the overall Cyber Security posture of an organization, since it is less likely an attacker has access to *both* of the required items. Other second-factors can be used including:

- Unique physical or biometric characteristics (e.g., fingerprint, facial or voice recognition)
- Receipt of a phone call
- Confirmation of location (e.g., in the office) via IP address

Requiring two "known" things (a password, and the answer to a question) is sometimes used, but has more risk since both may be known. Attackers are beginning to find ways to circumvent MFA defenses as well, so like many things, this is not a silver bullet and should be combined with other detection and impact mitigation techniques.

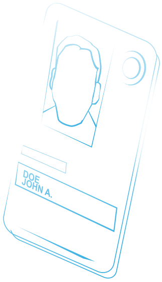
## What is IAM and why is it so important?



Identity and Access Managment (IAM) refers to the digital identification, with certainty, of an individual and the associated need-to know access to resources and information. Multifactor Authentication (MFA) provides a means to have authentication (you are who you say you are) that is much stronger than just a password that anyone could have. Role Based Access Control (RBAC) or Zero-Trust models provide authorization (you have access to the right things) strategies with differing levels of strength. Solutions like Single-Sign-On (SSO) allows users to authenticate once and have access to many things, which can help reduce security's perceived impact.

## What is encryption?

Encryption is ultimately a math equation that uses a “key” to transform digital information from plain text into jumbled text. Since these keys have to be very long, there is frequently a password used to protect access to the key. Encryption is only as strong as the password, key and algorithm. Assuming that a strong encryption algorithm is chosen, the most frequent attack against encryption is finding, or guessing, the password.
123456 as a PIN, anyone?



Encryption can be applied to the wrapper (e.g., the hard drive the data is on; the tunnel the data is flowing through) or to the information itself (e.g., the actual file or field). Symmetrical encryption uses the same key to perform encryption and decryption (similar to a door key). Asymmetrical encryption uses different keys for encryption and decryption (typically referred to as “public” and “private” keys).

## What is meant by “data-at-rest” or “data-in-motion”?

The term data-at-rest refers to inactive data stored in a powered-down data repository (e.g., a laptop that is off, a disconnected USB stick). This is frequently misused in the context of data on a server being "at rest", but since servers are rarely "off", the data is not "at rest" and encryption-at-rest solutions would not protect it. In these cases, file- or field-level encryption would be necessary to provide protection. Data-at-rest is typically most vulnerable when associated with portable devices (e.g., USB sticks, laptops or smartphones). Encrypting portable devices provides a high rate of return in risk mitigation, since it reduces the impact of device theft if proper encryption is employed on the device.

Data-in-motion refers to a stream of data moving from one place to another, whether through across the Internet (e.g., web traffic, email) or on an internal network. Similar terms to describe data-in-motion include “data-in-transit” and “data-in-flight”. Encryption of data-in-motion is commonly done with Transport Layer Security (TLS) or through a Virtual Private Network (VPN).

## Why aren't AI and Behavioral Analytics sufficient?

Unfortunately, some organizations mistakenly use automated security tools as a replacement for basic security measures and associated human resources. This misdirected concept of operation reduces the organization's security posture, and many times, results in an incident that could have been prevented had the focus been on implementing existing tools and techniques rather than trying to acquire and rely on automated tools.

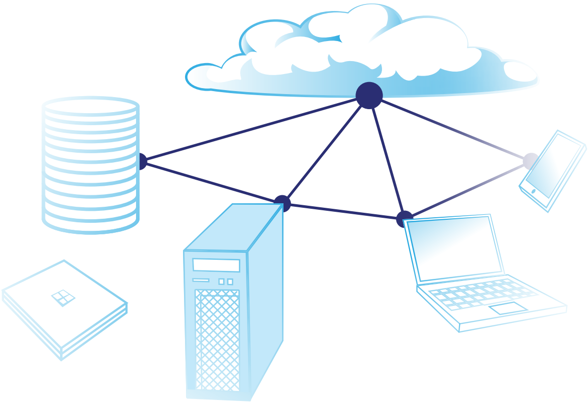
Automated security tools *can* assist security personnel in accomplishing their tasks by consolidating substantial amounts of security data and providing alerts when cyber events are identified as abnormal. However, the tools need to be correctly implemented, properly tuned, and *appropriately* monitored to ensure that attackers are not circumventing the controls. Similar to robotic technology used in human surgery, it is imperative that skilled personnel continue to provide oversight and ensure that basic measures and mitigation efforts remain in place.

## Why should non-IT executives be aware of Cyber Security measures?

IT's job is to make information available. Security's job is to make information unavailable (to attackers). The inherent conflict between these two creates friction between all parties. Additionally, IT teams provide critical input to, but are not the sole owner of, information systems. While IT personnel ensure data flows on demand to support the business, security options are frequently constrained by operations (not technology). Finding the proper mix between "secure", "accessible" and "usable" requires strong interaction and communication between the various teams.

Executives must help make risk-based decisions, asking pointed questions to data and application owners in order to adequately identify, account for and protect critical and sensitive data to the extent necessary. This is an area where IT is frequently instructed to "make it work", leaving potential gaps in security. When attackers access a system through one of these gaps, inter-connected solutions can be then be leveraged and exploited unless strong segmentation and detection controls are in place. Without water-tight doors, a flood in the bathroom can leak into the living room and beyond.

A tabletop exercise (TTX) is one way of increasing this overall awareness. This exercise is typically conducted with a combination of IT and non-IT participants, and addresses an possible attack scenario and its impact as a thoughtexercise instead of an actual event. Similar to disaster planning, a TTX provides an opportunity for all parties to ask questions and gain an understanding of the Strategic, Tactical and Operational components of various Cyber Security Measures and the over Incident Response process.



## Why would non-IT executives be part of a Cyber Security incident response?

There are many levels of participation for Cyber Security incident response, including:

- Legal
- Communications
- Operations

At the executive level, informed discussions must be made regarding the potential loss of significant data or the impact of compromised operations. Knowledge and comprehension of potential issues, possible solutions and mitigations, and the overall Cyber Security incident response process should be gained prior to an incident. This can be done as part of a Tabletop Exercise or other activity that allows dynamic discussion of the Strategic, Tactical and Operational considerations necessary when responding to an event.

## What are the potential repercussions of a data breach?

The impact of a cyber data breach varies based on the industry, size and type of organization; however, there are a few common impacts.

**Reputational damage:** Loss of customer and stakeholder trust is an intangible asset that is often very difficult to regain. Allowing the compromise of data confidentiality that was entrusted to your organization is a significant issue that can affect not only clients but also the ability to attract the best talent, suppliers and investors in the future.

**Monetary loss:** Direct and indirect costs to a business or organization can be crippling. The loss of business due to disruption, loss of intellectual property and years of effort and investment in research and development could potentially eliminate any competitive advantage in the market place. In addition, the cost of investigating and remediating a cyber incident is significant along with legal advice, potential customer notification requirements and public relations consultation which can exceed amounts covered by many cyber insurance policies.

Also, the conclusion that “reasonable” Cyber Security measures were not in place at the time of the breach can lead to fines from governmental and non-governmental agencies (e.g., Federal Trade Commission (FTC, Department of Health and Human Services (DHHS), Payment Card Industry (PCI)) as well as losses in legal action from impacted parties. According to the U.S, National Cyber Security Alliance, over 60% of small and medium sized businesses cease to exist one year after experiencing a Cyber Security breach.

# Thoughts & Takeaways

Is your organization adequately prepared and secured against today's and tomorrow's cyber threat?

- Do you have an Incident Response Plan (IRP)?
- Have you conducted a tabletop exercise (TTX) in the past year?
- Do you know how much data you have and how old it is? How often can you, should you, and do you "take out the trash"?
- Do you know where your data is? If it's "in the cloud" are you ready for thunderstorms?

# Other Resources

## Department of Homeland Security

www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

www.dhs.gov/news/2018/01/04/update-your-system-now-protectyourself-against-known-cyber-vulnerabilities

www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf

www.dhs.gov/stopthinkconnect-toolkit

www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

## Federal Bureau of Investigation

https://www.fbi.gov/investigate/cyber

## Federal Trade Commission

www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

## Securities & Exchange Commission

www.sec.gov/news/statement/cybersecurity-challenges-for-smallmidsize-businesses.html

## United Kingdom

www.cyberessentials.ncsc.gov.uk/

www.gov.uk/government/collections/cyber-security-guidance-forbusiness

→ **Contact Us Today!**

## Specialties

- Incident Response
- Cyber Security Solution Development, Testing & Review
- Digital Data Forensics Investigation & Analysis

## Background & Expertise

- Headquartered in Sarasota, Florida USA
- Clients include Fortune 500, Government, Public, Private, Regional and Law Enforcement
- 1 of 16 Companies Accredited by National Security Agency (NSA) and NSCAP for Cyber Incident Response Assistance (CIRA)
- 1 of 9 Companies Authorized to Investigate Card Breaches (PCI) in USA for VISA, MasterCard, AMEX: PCI Forensic Investigators (PFI)
- Expert Witnesses, Special Master of the Court (Criminal and Civil Cases)
- Intelligence Centric Methodology (NSA, DoD / Air Force backgrounds)