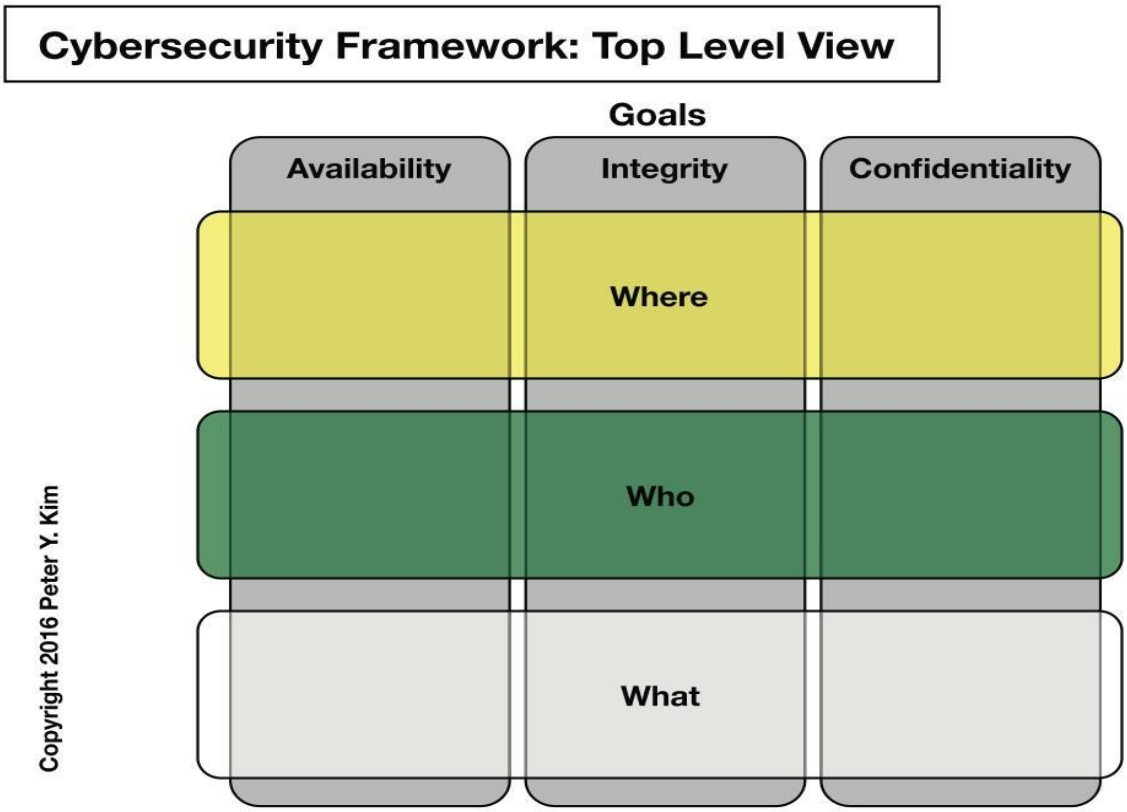
Cybersecurity Illustrated

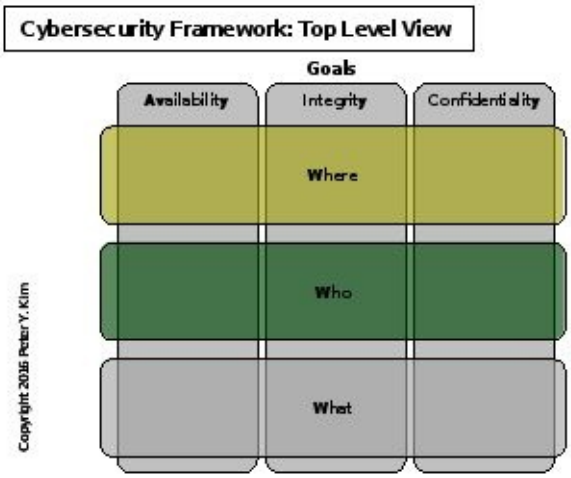
Just the Essentials (in just 2 hours)



Peter Y. Kim

Cybersecurity Illustrated

Just the Essentials (in just 2 hours)



Peter Y. Kim

ISBN: 1540591476
ISBN-13: 978-1540591470

The Purpose of This Book

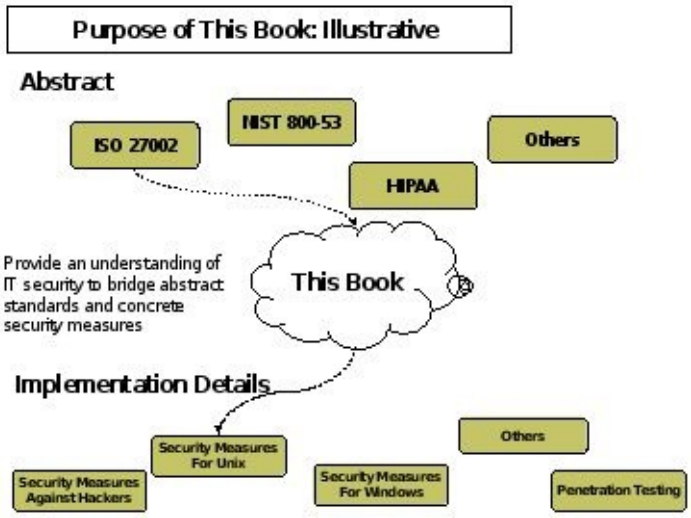
This book is for IT security professionals who have tried to use ISO 27002 and NIST SP 800-53, or compliance standards to start an IT security program but found them too generic and abstract to get started. This book fills the gap between those standards and specialized materials that detail security measures specific to malware, hackers, Unix boxes, Windows boxes, firewalls, web applications, and others.

The book provides examples to help you understand security issues that may apply to your organization. This book presents security measures in context so you can apply security measures in the right place for the right purpose.

An understanding of IT security will ease your understanding of compliance standards in the IT context because they – in a nutshell – require the implementation of IT security measures to safeguard particular kinds of data. Therefore, IT security is covered first and compliance second.

Many books and Internet resources detail specific IT security measures. This book does not replicate those materials. This book's goal is to help you build enough of an understanding of IT security so you can identify the security needs of your organization and know what specialized information you should pursue further.

Each lesson builds on ideas presented in earlier lessons, so reading them in order will help you get the most out of this book.



.

CONTENTS

Part 1: Understanding the Cybersecurity Framework

This part covers the Cybersecurity Framework, a framework that helps you view your IT landscape in terms of security issues. In the same way an army general must understand his terrain, the places he must protect, and his enemies when defending his territory, the IT professional must understand what he must protect and threats to his IT infrastructure. This part helps you identify your most important IT assets and threats that endanger their well-being.

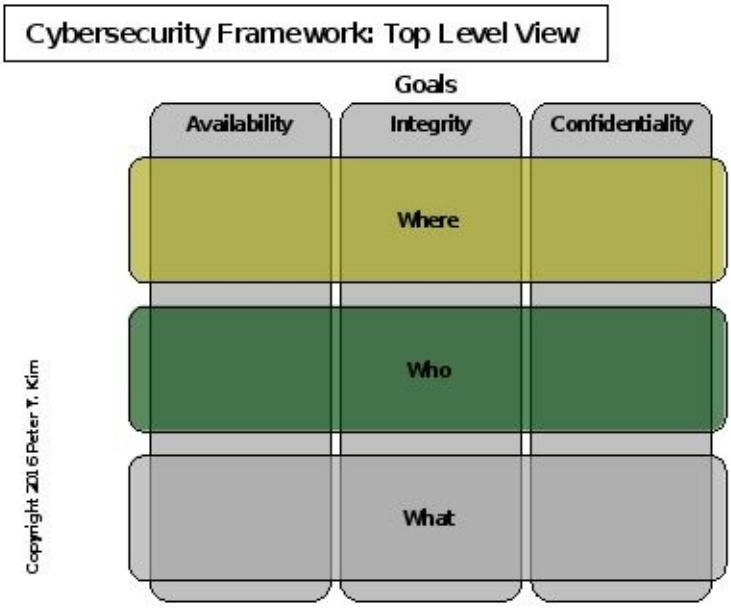
Lesson 1: Defining the Landscape of IT Security Issues - The CyberSecurity Framework

Introduction

This lesson describes a framework that IT professionals can use to navigate the landscape of IT security issues.

This framework defines:

1. Goals – Bad things that should be prevented
2. Where - Where bad things can happen
3. Who - Who can do bad things
4. What - “Non-people” things can do bad things



Goals – Three Security Goals

Many organizations share the following common goals:

1. Availability of IT Resources
2. Data Integrity
3. Data Confidentiality

Below are examples of failures in each.

Examples of Availability Failures:

1. Crashed email system hurts employee productivity.
2. Inoperative internal network prevents completion of backups undermining disaster recovery.
3. Downed web servers of e-commerce site prevent customers from making purchases and your company from earning revenue.

Examples of Data Integrity Failures:

1. Falsified financial data misrepresents your company's financial performance.
2. Modified patient records under/overcharge insurance companies.
3. Modified source code library leaves a security hole in enterprise software product.

Examples of Data Confidentiality Failures:

1. Credit card numbers are stolen from e-commerce website.
2. Design for new IC chip is stolen.
3. Stolen patient records betray patient privacy.

Where – Spaces and Assets

Physical and Logical Space

"Bad things" can happen in two different spaces: the **physical space** and the **logical space**.

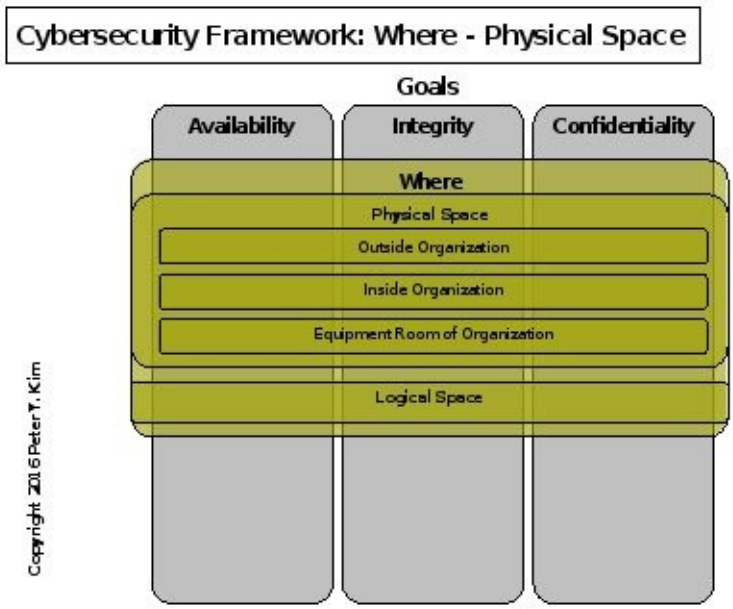
Physical space refers to the physical world. **Logical space** refers to the world inside networks and computers, the world of user accounts, passwords, and databases.

An example of a security incident in the physical space is someone physically stealing a computer. An example of a security incident in the logical space is someone breaking into a database account over the network and stealing confidential information.

Types of Physical Spaces

There are three types of physical spaces:

1. Outside. Everyone can be outside.
2. Your organization's office area. It holds people's personal computers and media. Within the general office area, your organization's internal network can be accessed.
3. Your organization's equipment room. It houses network equipment and shared computing resources.



Only select people can enter the office and even fewer are permitted to enter the equipment room.

Types of Assets in the Logical Space

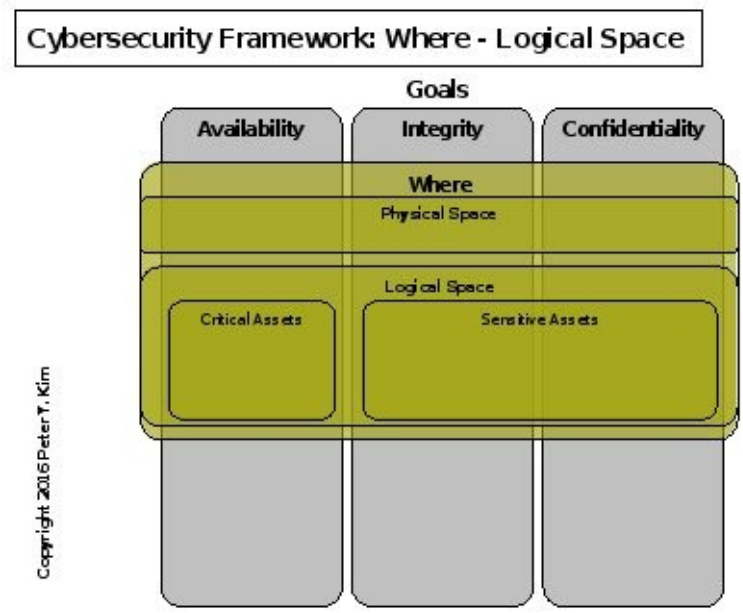
There are three classes of assets in the logical space.

1. Network Equipment
2. Shared Computing Resources including OS and software that reside on hardware
3. Personal Computing Resources such as desktops and laptops

It is helpful to distinguish each class because their usage characteristics differ and their surrounding security issues differ.

Two Asset Characteristics

There are two important asset characteristics: **criticality** and **sensitivity**. Unavailability of critical assets disrupts your organization's operation. Sensitive assets contain sensitive information.



Examples of Critical Assets

1. You run an online stock trading business. If your web servers crash, your customers cannot trade. Your web servers are critical.
2. Your email servers go down. Your employees cannot send/receive email. Productivity is hurt. Email servers are critical.
3. Your domain controllers go down and your employees cannot log into the network. Productivity is hurt. DC's are critical.

Examples of Sensitive Assets

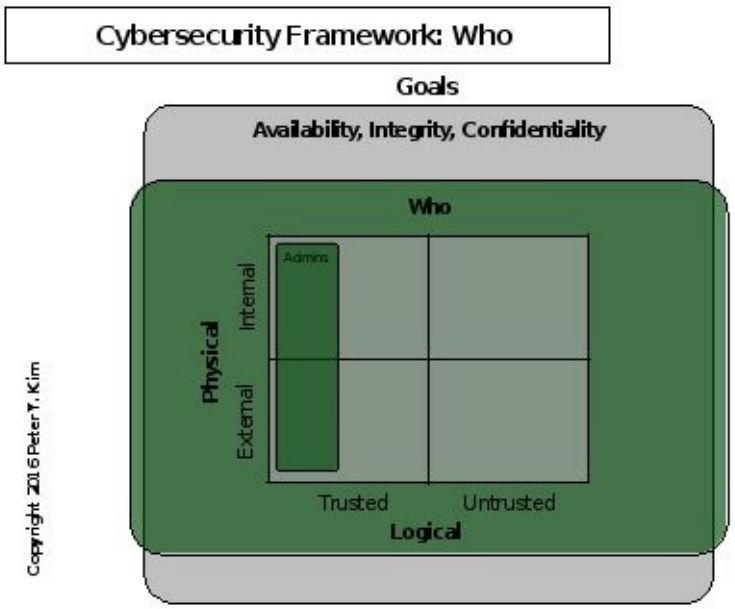
1. You have a public company. The database containing your financial data is sensitive because if someone falsifies financial data, you are misrepresenting your financial performance.
2. You run a healthcare provider. The database containing your patient identity information is sensitive because patient privacy must be protected.
3. You run a chip design company. The database holding the blueprints for the latest chip designs is sensitive.

Assets can be both critical and sensitive. For example, the unavailability of an electronic medical record system [EMR] can hurt a doctor's ability to treat patients and the system contains sensitive patient information. In this case, the EMR system is both critical and sensitive.

Critical and sensitive assets should be the focal points of your security measures.

Who – People

People are one cause of "bad things."



Distinguishing different groups of people in your organization is important because their surrounding security issues differ.

The first set of characteristics distinguishes people by their physical location and their logical "status."

1. **External vs. Internal:** People who work physically outside your premises vs. people who work inside.
2. **Trusted vs. Untrusted:** People who have accounts on computing resources vs. people who don't.
3. **Administrator vs. Non-Administrator:** People who are empowered with special privileges vs. people who are not.

A major security issue with untrusted users is allowing only the right people to become trusted users. For example, someone in the sales department can be mistakenly provided an account on a finance system although only people in the finance department should have access.

A major security issue with trusted users, especially administrators, is detecting the misuse of their privileges. An administrator responsible for maintaining a database can abuse his privileges and query out social security numbers from the database although he is not supposed to.

The following second set of characteristics defines people's "business roles." Depending on their business role, they will have access to different assets, and therefore, different security measures will apply.

1. Full Time Employee: People who are full time employees.
2. Customers: People who use your computing resources as customers.
3. Partners: People who access your computing resources as partners.
4. Consultants/Contractors: People who are not full time employees, but work for you.
5. Accounting, Sales, Engineering, Human Resource, etc.: People from different departments have access to different assets.

Combinations of characteristics can apply to a single person. Someone can be a trusted/internal full time employee with administrative powers who works for the finance department.

What – Non-People Related Dangers

Non-people things can cause “bad things” to happen. There are programmatic threats such as viruses, worms, and other malware that can undermine availability, data integrity and data confidentiality. Denial of service attacks also fall into this non-people category.

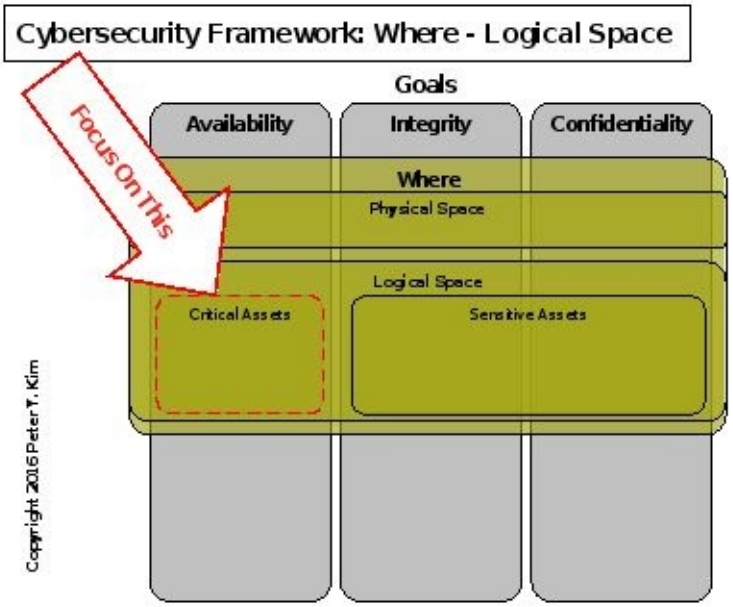
Vulnerabilities within your software are another danger. Vulnerabilities open opportunities for people and non-people to exploit and compromise availability, integrity, and confidentiality.

Conclusion

We now have a framework for discussing security issues. You know your goals, where you should focus, and who/what to protect against.

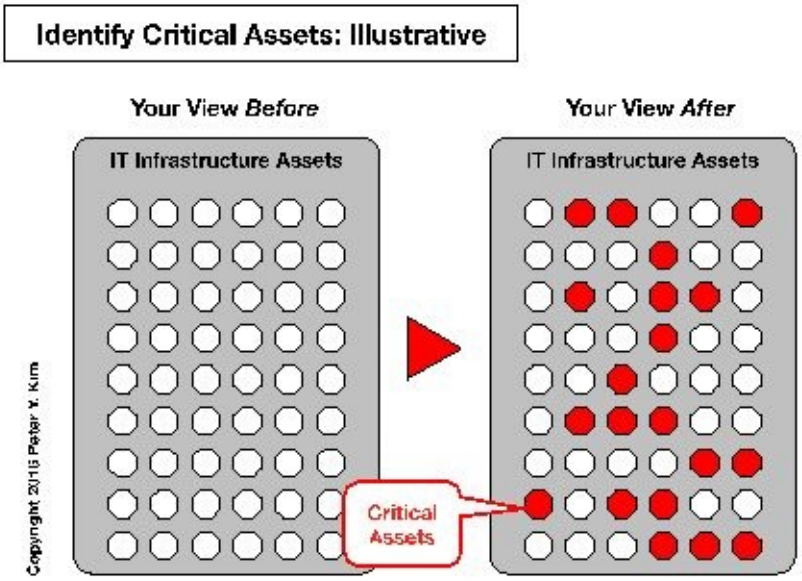
Lesson 2: “Where” of the Cybersecurity Framework – Critical Assets

Focus of This Lesson



Introduction

This lesson focuses on **critical assets** of the Cybersecurity Framework. Reading this lesson should help you identify your organization's critical assets, assets you must safeguard.



Identifying Critical Assets of Your Organization

The unavailability of critical assets disrupts your organization's operations. Security measures to safeguard availability apply to critical assets.

Each organization has different critical assets because each organization is different. A healthcare provider that uses only electronic medical records [EMR] and no paper records should regard its EMR system as critical because the unavailability of this system can obstruct the treatment of patients.

If the web servers of an e-commerce site are unavailable, customers cannot buy products on the site. Since customers can buy from another vendor, unavailability can mean lost revenue. Any subsystem that supports the proper operation of the e-commerce site is a critical asset.

To identify your critical assets, you should ask yourself, "The unavailability of which assets would cause my organization to feel immediate pain? … would hurt my organization in terms of decreased revenue or increased cost? … would hurt my money making capability? … would hurt my employees' productivity? … would block the way my organization gets its work done?"

Examples of Critical Assets

Walking through more examples can help you identify critical assets of your organization. The list is not meant to be complete.

Example 1: Any Company

It's hard to imagine a productive work environment without network connectivity. Network connectivity includes: connectivity of internal people to internal computing resources or to the Internet. It can also include connectivity of your mobile sales people to your internal computing resources. The network assets that support these connections are critical.

Example 2: Any Company

Your email server is probably a critical asset. Many people in your organization rely on email to communicate and get things done. Most emails might not need immediate attention but some may be urgent.

Example 3: Stock Trading Firm

The unavailability of a stock trading system for a few minutes may have large negative consequences to your business because you cannot perform trades that support your bottom line.

Example 4: Cell Phone Company

The unavailability of a CRM system may render your organization incapable of serving customers who call in for help. The data in the CRM system is critical because losing historical records of your customers will undermine the well-being of your business.

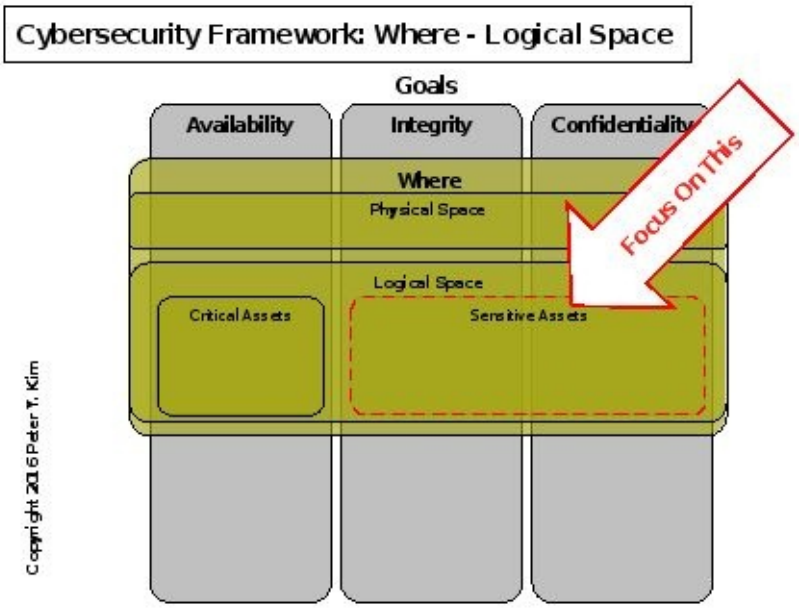
Conclusion

Critical assets are focal points of your security program.

The examples above should help you identify your organization’s unique set of critical assets and compile a list.

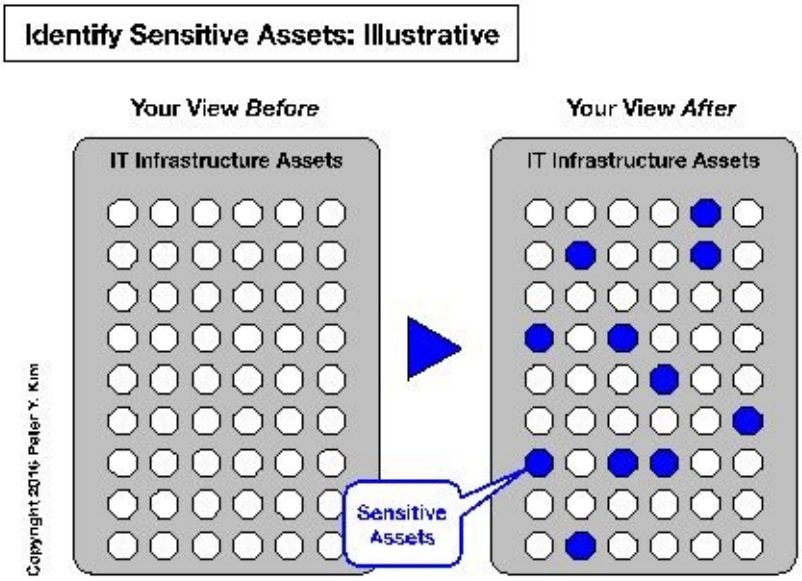
Lesson 3: “Where” of the Cybersecurity Framework – Sensitive Assets

Focus of This Lesson



Introduction

This lesson focuses on **sensitive assets** of the Cybersecurity Framework. Reading this lesson should help you identify your organization's critical assets, assets you must safeguard.



Identifying Sensitive Assets of Your Organization

Sensitive assets such as databases, applications, and file servers contain sensitive information. Security measures to safeguard data integrity and data confidentiality apply to sensitive assets.

Each organization will regard different data as sensitive. Examples of sensitive information are usernames/password pairs, credit card numbers and personal identity information. Username and password pairs provide thieves with unauthorized access to accounts. Credit card numbers can be abused to make purchases on someone else's dime. People can commit identity theft with people's identity information.

There are three types of sensitive information:

1. Information that is inherent to the operation of your IT infrastructure. Information such as username and password pairs can open unauthorized access to resources. Configuration information can be altered to harm operations. An internal network map can help hackers navigate your network.
2. Information tied to individuals such as credit card numbers and identity information that can be used for identity theft.
3. Information tied to the organization such as financial data, source code, strategy documents, and military intelligence.

Sensitive information differs across organizations. For instance, a software company should regard its source code as sensitive. The military should regard its top-secret information as sensitive.

To identify your organization's sensitive assets, you should ask yourself the question, "What information, if stolen or altered, can bring harm to people including employees, customers, and investors, and to the wellbeing of my business?"

Examples of Sensitive Assets

Walking through more examples can help you identify sensitive information of your organization. Sensitive assets contain sensitive information. The list is not meant to be complete.

Example 1: Any Company

Human resources data can include social security numbers, bank account numbers, and other employee information. This data is sensitive and its confidentiality must be protected because it can be used identity theft.

Example 2: Tax Paying/Public Company

Accounting data is sensitive because organizations have to report their earnings to file corporate taxes. Public companies must report its financial performance to its investors. You must protect the integrity of accounting data so that your organization files taxes correctly and accurately reports earnings to investors.

Example 3: E-Commerce/Online Payment Company

Many e-commerce/payment businesses store customer information such as name, web email address, password, physical address, credit card numbers, and bank account numbers. The confidentiality of customer data must be safeguarded. Since users often use a single password for all their accounts, the password for an e-commerce account may provide a thief with access to the customer's email account too.

Example 4: Computer Chip Company

Some information must be safeguarded for the well-being of your organization. For instance, the confidentiality of a new chip design must be safeguarded so no competitor can copy your work.

Example 5: B2B Company

A B2B company's clientele information is sensitive because competitors can use this information to steal customers away from you.

Conclusion

Identifying sensitive information helps identify sensitive assets that require safeguards. These assets are focal points of your security program.

The above examples show different types of sensitive data; some examples probably don't apply to you. However, you can think of parallels to the above example that are unique to your organization. You should be able to compile a list of sensitive information and assets of your organization.

Lesson 4: Using the Cybersecurity Framework to Understand PCI, HIPAA, SOX

Introduction

The Cybersecurity Framework can help us more easily understand the thrust of PCI, HIPAA, or SOX in the IT universe.

Let's review the "Goals" and "Where" of the Cybersecurity Framework.

Goals – Three Security Goals

There are three security goals:

1. Availability of IT Resources
2. Data Integrity
3. Data Confidentiality

Where – Sensitive and Critical Assets

There are two important asset characteristics: criticality and sensitivity. Unavailability of critical assets disrupts your business. Sensitive assets contain sensitive information.

PCI, HIPAA, SOX

The Cybersecurity Framework can help us more easily understand the thrust of PCI, HIPAA, and SOX. The following explanation is NOT meant to be a complete explanation, but an explanation of the IT security component of compliance.

PCI

PCI requires security measures to protect the *confidentiality* of payment card information. Assets that contain payment card information are sensitive assets that must be protected against theft.

HIPAA

HIPAA requires security measures to protect the *availability*, *integrity* and *confidentiality* of electronic "protected health information" or PHI. Assets that contain PHI are sensitive assets that require security measures.

SOX

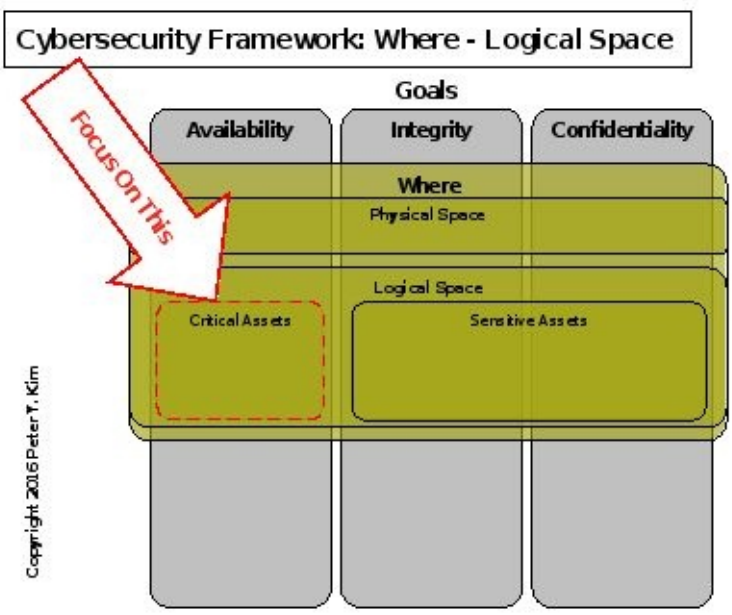
SOX requires accurate financial performance reporting. It holds executives responsible for the accuracy of their financial reports; they can go to jail for approving bad reports. Protecting the *integrity* of financial data is therefore important. Assets that contain financial data are sensitive assets that must be protected against tampering.

Conclusion

Now you can see that understanding IT security helps you better understand compliance requirements. If you understand security measures that address IT security goals, then you will have an easier time understanding the measures necessary to achieve compliance. PCI will pivot around payment card information, HIPAA will pivot around PHI, and SOX will pivot around financial data; however, each will use similar security principles to safeguard data.

Lesson 5: Gradations of Criticality

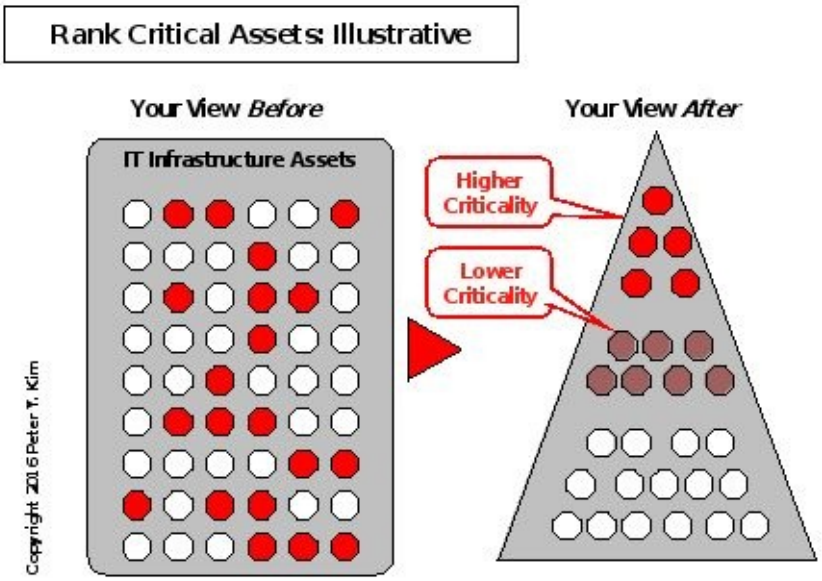
Focus of This Lesson



Introduction

A rank order list of assets by criticality or sensitivity can help your team prioritize their work. This lesson focuses on distinguishing levels of criticality. This rank order list is only one decision-making factor out of many others when allocating resources. Other factors include the ease of implementing the security measures and the efficacy of existing security measures.

Assessing criticality is more of an art than a science. This lesson suggests an approach to assessing criticality with a series of questions that can help you to create a ranking pyramid that groups assets into bands of criticality and rank order assets within their bands.



Questions to Assess Criticality

To assess the criticality of an asset, try to imagine it without redundancy or backup/recovery measures first. The higher the criticality of a system, the more you should be interested in implementing redundancy and backup/recovery measures.

The greater the negative impact of the unavailability of an asset is on your organization, the higher its level of criticality. Below are questions that help you size up the negative impact.

Questions to Assess Criticality

1. **Breadth**: If an asset becomes unavailable, how many people are negatively impacted? The larger the number, the greater the asset's criticality.
2. **Alternatives**: If an asset becomes unavailable, are there alternative ways to get the same work done? The more difficult it is to get the same work done, the greater the asset's criticality.
3. **Urgency**: If an asset becomes unavailable, how urgent are the activities that cannot be completed? The more urgent, the greater the asset's criticality. Is it always urgent? The greater the frequency of urgency, the more critical.
4. **Money Related**: If an asset becomes unavailable, how does it impact the organization's money-making operations? The less able an organization can earn money, the greater its criticality.

The combined answers to the above questions will give you a sense of the criticality of an asset. Some assets will be clearly more critical than others. Some will be difficult to rank higher or lower than others.

Bands of Criticality and Rank Ordering Assets

Going through the process of asking the above questions and grouping assets into bands of criticality is the first step. The highest band will contain the fewest assets that are of the highest criticality. Each lower band may have increasingly more assets. This basic grouping may be sufficient to get your security program started.

If necessary, you can proceed to rank order the assets within each band with the following procedure.

You can create a rank ordered list by comparing two assets at a time across the four questions and force yourself to decide which is more critical than the other.

Let's assume we have five assets in a band. Choose two assets and decide which is more critical than the other. Then take a third asset and make the same kind of comparison with the asset on ranked 1 in your list and the third asset. If you decide that the third asset is less critical then compare the third asset with the asset ranked 2. If the third is more critical than rank 2, then make the third asset rank 2, and what was originally ranked 2, rank 3. You can follow the similar steps with the remaining assets to complete a prioritized list. As you gain experience, this process will become quicker.

I can provide you with a scoring system that rates criticality, but this system would be arbitrary and your organization may be worse off relying on my arbitrary formula for ranking your assets than using the approach described above.

Examples of Assessing Criticality

Below are examples that demonstrate the above approach at fictitious organizations.

Example 1: Assets that Support the Internal Network At An Enterprise Software Company

1. **Breadth:** Everyone is affected by a downed internal network. Both internal and external people cannot access internal resources.
2. **Alternatives:** The phone is an alternative to email for the sales team and a few other people; the majority rely heavily on email and the phone is not a workable alternative. The customer support team has no alternative to their electronic knowledge database. Engineering has no alternative of getting latest source code.
3. **Urgency:** The customer support team cannot serve customers effectively without immediate access to electronic knowledge database. Engineering cannot check in or check out new code, but they have enough to do on their personal computer to not need access to newest code immediately.
4. **Money Related:** The relationship with revenue is distant. Customer satisfaction is undermined so revenue may be hurt in the long run, but it does not immediately impact the bottom line. Engineering's idle time may increase costs.

The criticality of the internal network is higher than most other assets at the company.

Example 2: VPN Assets At The Same Enterprise Software Company

1. **Breadth:** People working externally from home office or sales people who are on the road are affected. 15% of the work force is external.
2. **Alternatives:** External people can decide to go to the office, but going to the office is not a viable alternative for most. Sales people can use the phone.
3. **Urgency:** People working from home have some work to do already on their home computers. Sales people already have most of their sales materials on their personal computer.
4. **Money Related:** People are idle and productivity is decreasing, so cost is increasing. Revenue loss is unlikely.

The criticality of the VPN system is high, but not as high as assets for the internal network at this company because breadth of impact is lower. In terms of the other dimensions, alternatives, urgency, and money related-ness, the two assets might be about the same. Using this kind of comparison between assets can help you rank order your assets.

Example 3: Online Shopping Website For An E-Commerce Company

1. **Breadth:** Your organization as a whole is affected.
2. **Alternatives:** Your organization does not offer other ways customers can place orders.
3. **Urgency:** Although some loyal customers will wait for your service to recover,

most will buy elsewhere. Every minute of downtime means that you lose revenue.

4. **Money Related:** This asset is directly related to your organization's ability to generate revenue.

The criticality of assets that support the online shopping site is very high for this organization.

Conclusion

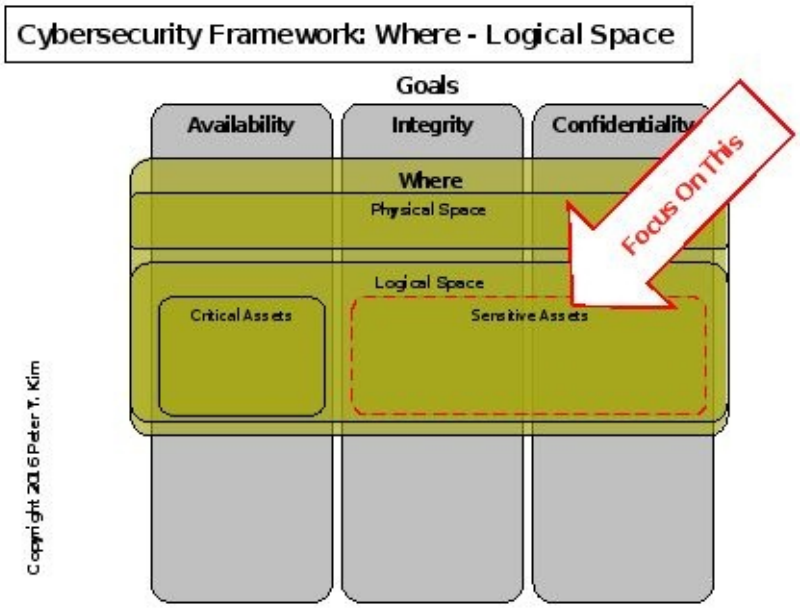
You now have an approach to rank order assets by criticality.

Creating a rough rank ordered list is a good exercise for you and your team. Once you have reviewed your critical assets with the above approach, your team will have an opinion about which assets are more important than others, and use this as one factor in prioritizing the implementation of security measures.

You will inevitably change your mind about the ranking as you rethink the answers to the four questions and something new occurs to you.

Lesson 6: Gradations of Sensitivity

Focus of This Lesson



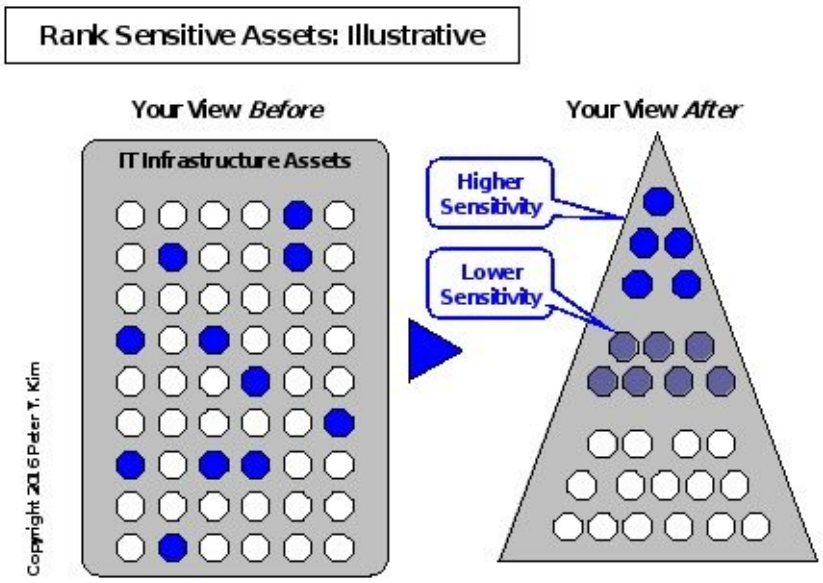
Introduction

A rank order list of assets by criticality or sensitivity can help your team prioritize their work. This rank order list is only one decision-making factor out of many others when allocating resources. Other factors include the ease of implementing the security measures and the efficacy of existing security measures.

A previous lesson helped you identify your critical assets. This lesson focuses on distinguishing levels of sensitivity.

Assessing sensitivity is more of an art than a science. This lesson suggests an approach to assessing sensitivity with a few questions that can help you to create a ranking pyramid that groups assets into bands of sensitivity and rank order assets within their bands.

Sensitive assets hold sensitive data. Sensitive assets often are databases on shared computing resources. The more sensitive the data is, the more sensitive the asset is.



Questions to Assess Sensitivity

To assess the sensitivity of an asset, try to imagine it in isolation without the benefit of any protection such as Data Loss Protection. This will help you separate the sensitivity of an asset from the security measures that protect the asset. Furthermore, separate out the efficacy of the post-incident response plan. The more sensitive the asset, the more interested you should be in implementing measures to quickly detect and respond to security incidents around the asset.

The greater the negative impact of the tampering or theft of sensitive information is on your organization, the higher the sensitivity of the asset containing it. Below are questions that help you size up the negative impact.

Questions to Assess Sensitivity

1. **Breadth:** If data within the asset is altered or stolen, what is the breadth of the negative impact? How many people are negatively impacted? The larger the number, the greater its sensitivity.
2. **Depth:** If data within the asset is altered or stolen, what is the depth of the negative impact? Will your organization be fined? Will people be sent to jail? Will people die? Will your organization be less secure? Will your organization's reputation be damaged? Will the competitiveness of your organization be compromised?

The depth of the negative impact varies widely depending on what the sensitive information is and what is done with that information. Therefore, it is difficult to summarize the sensitivity of an asset with a single rating.

It is easy to say that larger fines are worse than smaller fines. The loss of two lives is worse than the loss of one. But how do you compare something less tangible and quantifiable like the competitiveness of your organization to a fine? Another factor that influences these comparisons between money and lives is your organization's values. What is human life worth in terms of dollars?

There's usually some way to quantify these fuzzy damages, but the method must be hand crafted for each situation, so I will not cover this topic in this book.

Sometimes even after a thorough quantification using probabilities and consequences with the help of consultants, you'll only be marginally more confident that the resulting rank order is right. So spending an enormous amount of resources to create a perfect sensitivity ranking is dubious. However, going through the exercise described in this lesson should help you better understand the sensitive assets that you should worry about.

You can take a similar approach presented for criticality in the section "Bands of Criticality and Rank Ordering Assets" in the previous lesson. Quantify when you can or use your "common sense" to place sensitive assets into bands.

Examples of Assessing Sensitivity

Below are examples that demonstrate the above approach.

Example 1: Theft of Passwords for Company Email System of Any Company

1. **Breadth:** All can be affected.
2. **Depth:** Emails of executives can contain confidential information. Furthermore, a person's passwords for other resources are probably the same as the person's email password. Other resources can be compromised. Furthermore, the password of an administrator can be used to cause greater damage.

Stolen passwords can provide unauthorized access to not only email but also other applications. In general, sensitivity of passwords is high because the consequences can be extremely negative.

Example 2: Theft of Credit Card Information from E-Commerce Company

1. **Breadth:** All customers can be affected. E-commerce company is affected. Credit card company is affected.
2. **Depth:** Customers may be inconvenienced. E-commerce company can be fined by credit card company. Customers can stop shopping at E-commerce site.

The consequences of stolen credit card numbers can be large; however, in general, password information can be considered more sensitive because it can ease the theft of credit card numbers and other sensitive information.

Example 3: Alteration of Financial Data for Public Company

1. **Breadth:** Investing public, inside investors, the company as a whole, the company's executives can be affected.
2. **Depth:** Company executives can go to jail. Misled investors can lose large amounts of money.

If your organization is a public e-commerce company, then it's hard to determine which is more sensitive: financial data or credit card information.

If you must allocate resources to implement security measures between the two, you may have to rely on other factors and not just the sensitivity ranking to make your decision. For instance, you may consider ease of implementation of security measures. Furthermore, you may consider the security measures already in place. Is one asset far more vulnerable than the other?

Example 4: Theft of Medical Records at Healthcare Provider

1. **Breadth:** The healthcare provider as a whole can be affected. Patient privacy can be violated.

2. **Depth:** Healthcare provider can be fined. Patient loses privacy.

Again, you can be fined for not taking proper measures. If medical records of celebrities are stolen and made public, then the consequences to your organization's reputation may be large. If you are a public healthcare provider, then the sensitivity ranking between financials and medical can be challenging.

Example 5: Theft of Chip Company's Blueprints of Proprietary Technology

1. **Breadth:** The company as a whole can be affected.
2. **Depth:** Competitiveness can be undermined. Revenue can be undermined.

Depending on what the blueprints are, the consequences can be large. If the information reaches competitors who can reproduce copies or follow similar designs, then your company's technological advantage is undermined.

Conclusion

We now have an approach to rank ordering assets by sensitivity.

Creating a rough rank ordered list is a good exercise for you and your team for the same reasons for going through the parallel exercise with criticality. Once you have reviewed your sensitive assets with the above approach, your team will have an opinion about what is more important than others and use this list as one factor in prioritizing the implementation of security measures.

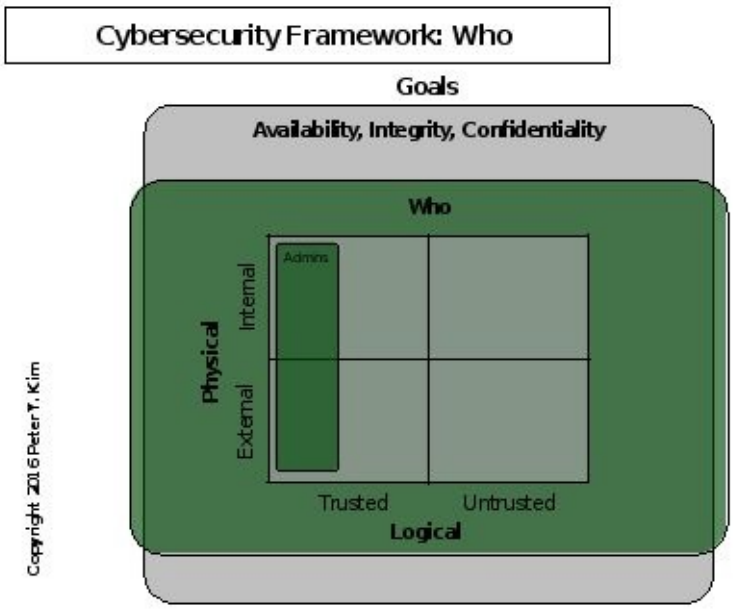
Completing this exercise for both critical and sensitive assets will help you get a good feel of the assets that you should worry about. Instead of a view of vast ocean of IT resources that appear equally important, you should now see your IT infrastructure with important areas and feel the weight of their importance.

Lesson 7: “Who” of the Cybersecurity Framework

Introduction

In an earlier lesson, I introduced the concept of “Who” in the Cybersecurity Framework. “Who” refers to people. This lesson provides more details about the importance of the following set of characteristics for people.

1. External vs. Internal
2. Trusted vs. Untrusted
3. Administrator vs. Non-Administrator



External vs. Internal

"External" and "internal" characteristics refer to the physical space. People who are outside the physical boundaries of your office are classified as "external." People who are inside the bounds of your office are classified as "internal."

This distinction is important because someone who is "external" has access to different resources than someone who is "internal." People can be "external" at one point in time and "internal" in another. A sales person is external when he travels and internal when he's visiting the office. But most people are one or the other.

The following are things that "internal" people might have that "external" people often don't.

Access to internal wireless or Ethernet network

1. Access to personal computers that have direct access to internal critical and sensitive assets
2. Access to people whom you can influence to acquire information or access
3. Access to people's workspace with documents with sensitive information (e.g. a slip of paper with a password)
4. Visual access to people typing in their password

There are potential security holes in the physical space of the "internal" environment that "external" people cannot leverage. External people are largely constrained to attack assets that are exposed to them in the logical space. The easiest path to compromising security is different for "internal" and "external" people.

Trusted vs. Untrusted

"Trusted" and "untrusted" users refer to users who have or do not have accounts in the logical space. Again, the vulnerabilities exposed to "trusted" and "untrusted" people are different.

For example, Kim has a web trading account with StocksRUs. David does not. Kim has access to StocksRUs web screens, so she can find vulnerabilities within the web application. David won't have access to the web trading screens' vulnerabilities.

Here's another example. Joe, an employee of ABC Co. has access to his company's accounting system, but not Mary, who is also an employee. Joe will have an easier time viewing confidential accounting information or inputting false records into the accounting system than Mary will have. Security measures for Mary with respect to the accounting system will be different from Joe's.

Administrator vs. Non-Administrator

Administrators are a subset of “trusted” people. It is important to distinguish administrators from non-administrators because administrators have many privileges that can be abused. For instance, a database administrator can use his privileges to query out credit card information although he should not be doing it.

Conclusion

Understanding the “Who” of the Cybersecurity Framework puts security issues in sharper focus. Security measures can differ not only because you are addressing different security problems of availability, integrity, and confidentiality, but also because you are taking security measures against different people. With a clearer sense of who you are guarding against, you can apply more specific and effective security measures.

Part 2: Security Measures

We can use the Cybersecurity Framework as a structure to cover the variety of security issues that must be addressed.

First, I will discuss different types of security measures and their common themes.

Second, I will discuss security measures that address components of the Cybersecurity Framework:

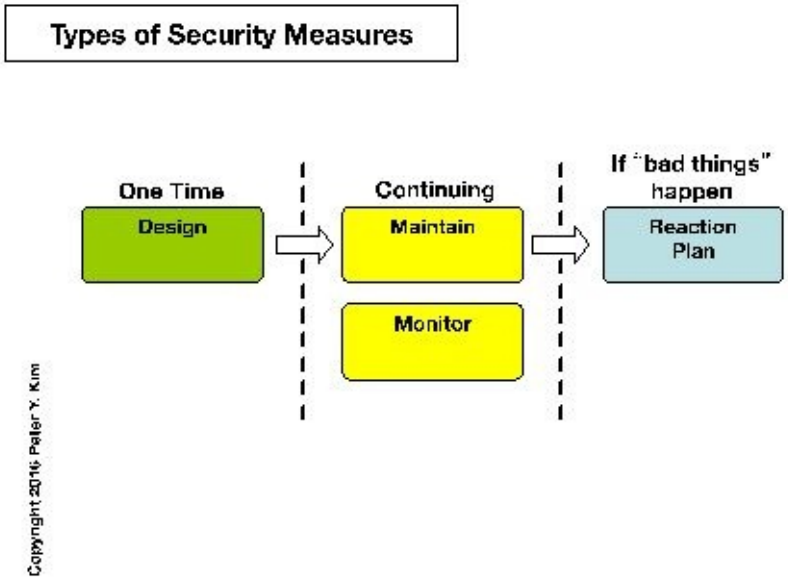
1. What
2. Where – Physical Space
3. Where – Logical Space

This part of the book helps you develop your vision of security measures. When evaluating security products, you will be able to think critically about how they fit into your vision and requirements.

Lesson 8: Types of Security Measures

Introduction

This lesson defines types of security measures.



Secure A Fortress

Drawing an analogy between guarding a fortress and guarding your IT infrastructure can help you more easily understand the types of security measures that can be taken.

1. Measure - Design

A fortress must be designed and built to keep bad guys out. Fortresses have only a few entrances that can be easily monitored and high walls.

2. Measure – Maintenance/Monitoring

The job of keeping the bad guys out does not end once the last brick is cemented into the fortress. The fortress receives regular inspection so any newly discovered weaknesses, like a crack in the wall or a broken lock, are repaired.

Furthermore, guards monitor the walls at night because a determined invader can climb the fortress walls.

Educating the entire population who reside in the fortress to report anything suspicious to the proper authorities can enhance security.

3. Measure - Reaction Plan

If guards, during their patrol, discover evidence that someone unwanted has entered the fortress then the guards must try to catch the intruder.

Secure Your IT Infrastructure

Now let's discuss what design, maintain/monitor, and reaction plan measures you can take to defend your IT infrastructure. Design measures are usually one-time setups, and maintain/monitor measures require continued action. Reaction plans must be prepared when something bad actually happens.

When addressing a security problem involving criticality, integrity, or confidentiality, you should consider measures across these broad categories.

1. Measure – Design

Just as you must design the fortress to be difficult to penetrate, you can design your physical space to be difficult to penetrate by installing door locks to entrances to your office and your equipment room. Provide keys to only the right people.

Within the logical space, you can design the topology of your IT network so that only the right people gain access to the right parts of the network. Furthermore, you can restrict logical access to applications by providing user accounts to only the people who should be accessing particular applications.

You can use technology to encrypt your sensitive data so that only people with the right permission can view the data.

There are measures that fall into both the physical space and logical space. Building redundant hardware and software assets to protect against hardware failure is one example. Having a system that backs up critical data can be another measure.

2. Measure - Maintain/Monitor

Many design measures require continued maintenance because circumstances change.

New evil software are born so you need to continue to update your antivirus software. Furthermore, new vulnerabilities are being discovered so you need continue to patch software with the latest vulnerability patches.

Because new people can enter your organization and old people can leave, you need to continue to make sure that the right people have access to the equipment room and the right people have accounts to the right applications.

You may also choose to monitor who is entering the office or the equipment room with a security guard during office hours and a camera that monitors the doorways or snaps a photo whenever someone unlocks the door during closed hours.

You can monitor the creation of accounts in your computers and applications so that you know that bad accounts are not being created.

You can monitor that your backups are being properly performed.

You can also inculcate safe IT security practices into members of your organization by periodically promoting habits that enhance security.

3. Measure - Reaction Plan

When something fishy is detected, you should have a human organization ready to create a reaction plan. Having a clear go-to person for reporting potential compromises can ensure that suspicious activities are addressed.

When availability of your critical assets is compromised, you should have a plan to return the assets to production. A “tried and true” plan to restore data from backups should be in place.

Because of the wide variety of damage that can result from compromises of integrity and confidentiality, it’s not practical to have a “tried and true” reaction plan in store for every possibility. You can, however, appoint someone as the go-to person for reporting compromises, so that your organization can react quickly.

Implementation of Security Measures

The technology for implementing security measures can be developed by your team, bought from a vendor, or downloaded freely. If you are going to use freely available tools, please use proper precautions to ensure that the tool is what you expect it to be and not malware.

If you are buying from a vendor, make sure you know what your requirements are first. Try to understand how vendor products fit into your requirements. Buying an expensive but cool security technology and counting on figuring out how to use it later will result in failure more often than not.

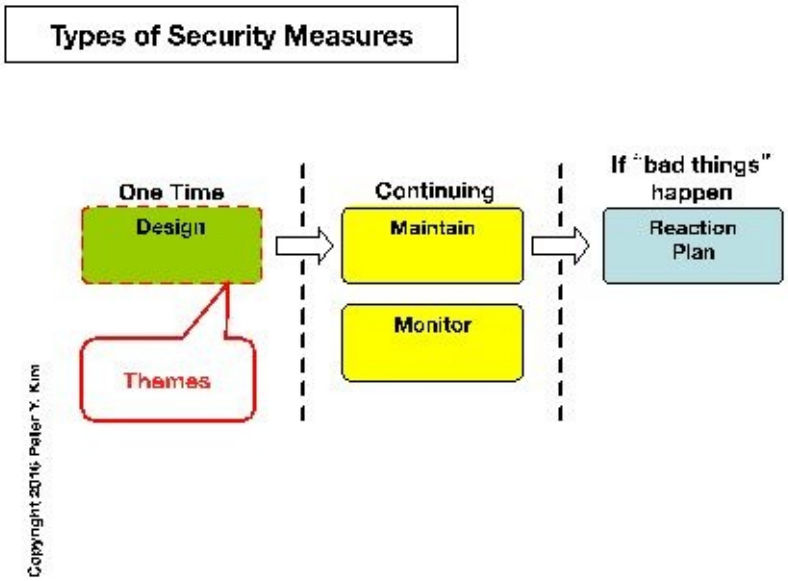
Conclusion

Now we know that there are three types of security measures:

1. Design – Set up your IT infrastructure the right way.
2. Maintain/Monitor – Maintain your design measures. Monitor to ensure that infrastructure is working as expected and there are no anomalies.
3. Reaction Plan – Formulate a recovery plan for critical failures. Create a team that server as the go-to contact for reporting incidents so your organization is ready to react quickly.

Lesson 9: Themes of “Design” Security Measures

Focus of This Lesson



Introduction

Minimization and uniformity are often themes that are considered good practices. This lesson provides examples to illustrate the concepts.

Minimization

Enhancing security through minimization is best explained through examples.

Account Management Example

Only provide accounts to people who need them and remove unnecessary accounts. Providing accounts to people who request it without verifying their need can result in accounts being given to the wrong people. Remove accounts of people who no longer need them. Accounts of people who left the company can be hijacked without the knowledge of the organization.

Account Privilege Example

Only provide privileges that are necessary. For instance, grant privileges that allow deletion of your organization's data from a critical application's database to very few people if at all. This protects against trusted administrators going "rogue."

Confidential Data Example

Do not store sensitive data that you do not need. Keeping around sensitive data only increases the probability of breaching confidentiality. Do you need everyone's physical mailing addresses in Active Directory for everyone to see? Mailing addresses can be used for identity theft.

Services on Externally Facing Computers Example

In externally facing assets, have the minimum number of active ports. A computer that hosts a web server might only need http and https ports open on the external network connections. If these are the only two ports that are open, do you need a firewall between the Internet and the computer? Perhaps not. If you choose not to have a firewall, then there's one less equipment to manage. You save money by not buying equipment and not spending time configuring it.

Uniformity

Vulnerability Patching Example

Having many one-of-a-kind computers can undermine your ability to automate patch roll out. Patches may install correctly in some but not in others because of differences in their configuration. Manual patching is a time consuming process and can leave your computers vulnerable for too long. Uniformly configuring computers can make patch roll out easier; if the patch installs successfully, then the identical process can be used to patch sister computers. This process can be automated with the use of patch management software.

Data Loss Protection Example

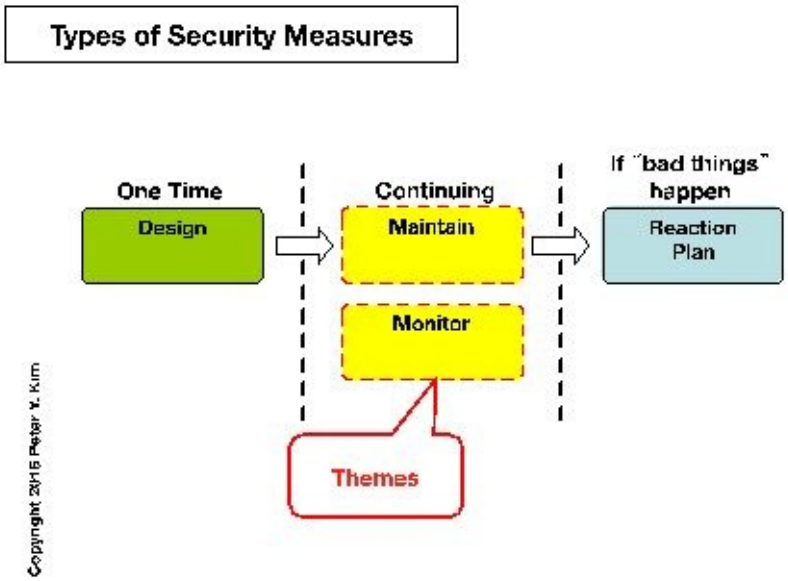
DLP products may require an agent to be installed on everyone's personal computers. The successful roll out of the agent may rely on the uniform configuration of everyone's personal computers. Installation of the agent may fail if the user has changed the personal computer's configuration drastically from the norm. If the configuration on personal computers is kept the same, the roll out may be easier.

Conclusion

Minimization and uniformity are two themes to consider when designing your IT infrastructure. These concepts will be revisited later in the context of the Cybersecurity Framework.

Lesson 10: Themes of “Maintain/Monitor” Security Measures

Focus of This Lesson



Introduction

This lesson discusses a variety of topics surrounding “Maintain/Monitor” security measures.

What You Can Monitor Depends On Your Data Source

There are two general approaches to monitoring application activity:

1. Use native logs (e.g. syslog, audit log) as sources of information.
2. Use an additional program that provides information that is not recorded in "native" logs.

The level of detail of logs can be set by setting the log's audit level. Even if a log is generated at the highest level of detail, the log still may not provide all the information that you desire. For example, a failed logon to a fileserver may be recorded but the reason for the failure might not be available in the log. A log file may tell you that the permissions of a file changed but it might not tell you what it changed from or who changed it. A database audit log might not tell you which user on a web application queried out sensitive information from the database.

When information in native logs is insufficient, you must develop a program, find a freely available program, or purchase a product that can creates the necessary information.

You should also be aware that a log that generates the information you need will generate lots of other information that you do not need. You may generate an overwhelming amount of information that no tool can effectively process to extract the events that you need.

Use Snapshot to Snapshot Comparisons If A Continuous History Is Unavailable

Identifying differences in data between two points in time can be one tool to monitor data integrity if a continuous change history is not available. One weakness to this approach is that data can be changed temporarily to fulfill a harmful purpose and then reversed between the two points in time that snapshots are taken.

This approach can be taken to monitor anything from user accounts that were added or deleted, to journal records in general ledger accounting systems.

Let Urgency Determine Periodic vs. Real-Time Monitoring

Monitoring can be done in real-time or periodically. Depending on what you are monitoring, you may want to be notified immediately with an alert when something fishy is detected. In other cases, periodic reports may be sufficient.

For instance, you may want to be immediately notified about a failure to backup critical data. However, you may not need to know immediately when a dormant account, an account that nobody has used in 90 days, is discovered. A weekly or monthly clean up of dormant accounts may be sufficient.

Strategies For Detecting Anomalies

Anomaly means irregularity from the norm. You can detect anomalies across a variety of dimensions such as logical location, physical location, and time band.

Logical Location

The Norm: John always logs in from his computer.

Anomaly: John logs in from Debbie's computer.

Physical Location

The Norm: John should be accessing computing resources from one geographic location at one point in time.

Anomaly: John is accessing his company's customer database from the office in Palo Alto and a company file server from his home in San Francisco. There's probably a second person who is not John accessing the company's resources.

Time Band

The Norm: Network maintenance is only done between 7am-8am on weekdays.

Anomaly: John logs into a router and changes its configuration outside the time band set by company policy. It might not be John making changes to the router.

The Norm: An automated batch job is done every first Monday of the month starting 1am with a designated service account.

Anomaly: Someone logs into the service account out of the usual time band.

Frequency

The Norm: Usually, John accesses four different applications per week.

Anomaly: This week, John has tried to access 16 different applications, half of which he does not have an account on.

The Norm: An average user downloads company's proprietary intellectual property files at a rate of two files per week.

Anomaly: John downloaded 20 files in the last week.

White List/Black List

The Norm: John uses the intranet search engine to find relevant information.

Anomaly: John, someone who has nothing to do with “Project XQ” the company’s super secret strategic plan, searches for the black listed term “Project XQ.” John should not be seeking this kind of information.

Avoid False Positives

The purpose of monitoring is to detect something “fishy.” Once something is detected, you must investigate it to determine whether what you detected is an indicator of something harmful going on. You must be choosy about what you monitor to avoid putting too much time into investigating false positives.

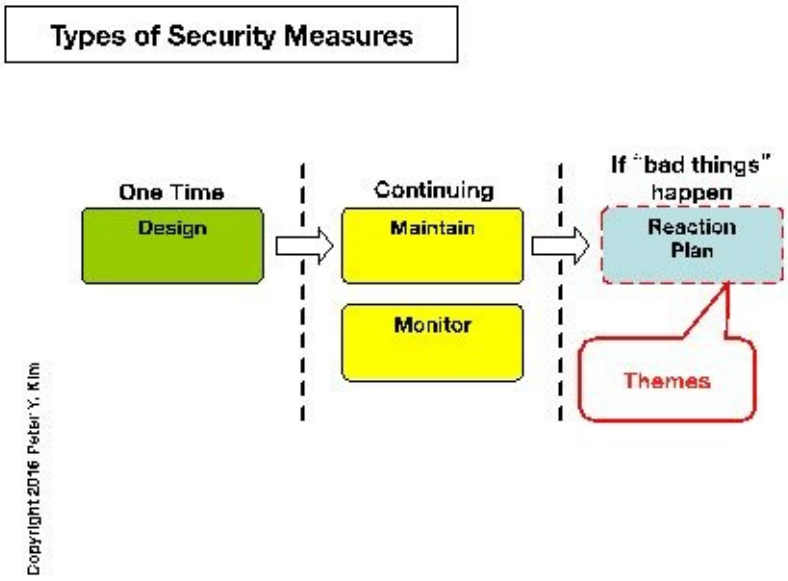
If your gut feeling is that certain security measures will lead to too many false positives, do not invest time in creating it. If a security measure that you thought would be effective is triggering too many false positives, then consider revising the measure.

Conclusion

These topics will be revisited later in the context of the Cybersecurity Framework.

Lesson 11: Themes of “Reaction Plan” Security Measures

Focus of This Lesson



Introduction

This lesson discusses the most important elements of “Reaction Plan” security measures. Planning for all possibilities is impractical. However, having a few measures in place can improve the efficacy of your IT security program.

Have A Critical Data Recovery Plan

Critical data can be lost from hardware breakdown, intentional/unintentional human action, or catastrophes. Using technologies such as RAID and high availability can safeguard data against loss from hardware breakdown, but they do not protect against human actions or catastrophes. Therefore, it is important to have a data recovery plan to address these dangers.

The loss of critical data such as customer data at an e-commerce company or source code at an enterprise software company can do irreversible harm. Having a recovery plan in place can safeguard your organization against disaster.

The recovery plan should be tested end to end, from taking the backup to restoring critical data using the backups. You do not want to discover that there's a glitch in the backup process that prevents full data recovery AFTER you have lost critical data.

Train Your IT Security Team to React

When your IT security team discovers something fishy is going on, then the team should know what to do next. Having an agreed upon process and the human organization to support the process will better ensure that potential security breaches do not go unaddressed.

The following is a generic process that can help you get started:

1. Notify proper authorities of potential security breach
2. Investigate whether there has been a security breach
3. Report findings to proper authorities
4. Agree on and execute next steps

Next steps can be immediately blocking harmful actions of a user, disciplinary action of an internal employee, monitoring the wrongdoer to do more to collect more evidence of wrong doing against him, correcting the damage, and redesigning security measures. Next steps depend on the particulars of the situation.

Designating someone as a collection point for all potential security breaches can ease reporting. This person can also be responsible for leading the creation and execution of a plan if investigation reveals that there has been a real security breach. This person will not work alone but collaborate with the owners of the breached asset and the IT team. For example, the security breach of an accounting system will require the notification of the head of accounting so that relevant people are involved in addressing the security issue. The IT team supports investigation and remediation.

Having a perfect process and organization completely planned is probably not worth your investment in time. Relying on your IT team to use their own judgment and following the rough process above may be enough to get the job done.

Encourage Your Organization to React

Fishy things can be detected not only by the IT security team but any member of your organization or even partners and customers. Anyone using your computing assets should be encouraged to notify the proper authorities when something fishy is detected.

Having a designated contact point to report all fishy things can facilitate the process of reporting potential security breaches. Informing everyone about availability of the contact point and encouraging people to use it can reduce the chances that security breaches go unaddressed.

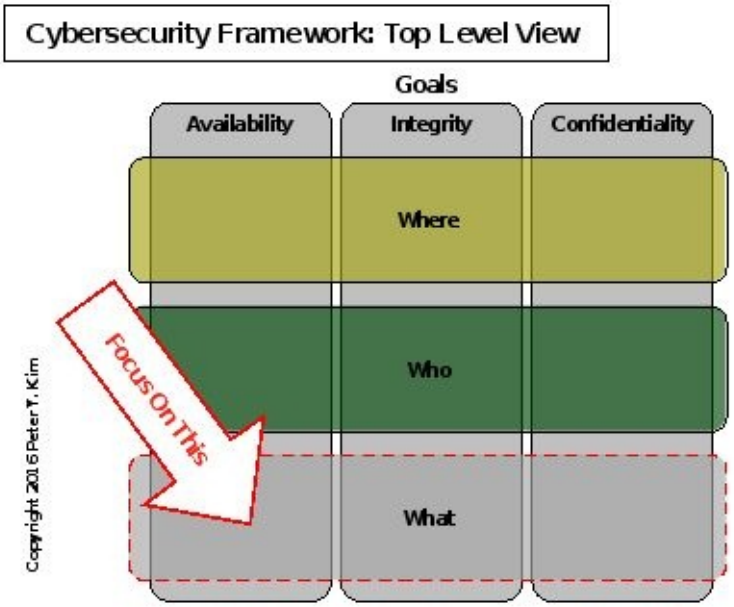
Conclusion

Having a tried and true data recovery process protects organizations against loss of critical data. Furthermore, encouraging people to react to fishy things is important so that potential security issues do not go unaddressed. Having clear channels to communicate concerns and initiate an investigation process improves probability of discovering and addressing security breaches.

These topics will be revisited in the context of the Cybersecurity Framework.

Lesson 12: Security Measures for "What" of the Cybersecurity Framework

Focus of This Lesson



Introduction

This lesson discusses the “What” component of the Cybersecurity Framework and the security measures that should be used to address them.

Evil software, such as viruses and worms, can undermine availability, integrity, and confidentiality. Evil software can be programmed to do arbitrary things that can harm your systems.

Furthermore, software vulnerabilities in your computing resources can be exploited by people or by programs to ultimately impact availability, integrity, and confidentiality. New vulnerabilities are always being discovered and being patched by software makers. Because new evil software continues to be born and new vulnerabilities are discovered, your security measures will involve continuously patching vulnerabilities.

Detailed documents about running vulnerability management programs are available on the Internet. This lesson won’t reproduce those documents but provide a nutshell summary of approaches.

Security Measures Against Evil Software

Use of antivirus and other anti-malware software is a measure that reduces the likelihood of IT trouble. There are many products that address systems that are often targeted by evil software. Implementation using these products may not be as challenging as the implementation of other measures.

Ideally, your security measures should do the following:

1. Protect your critical and sensitive assets especially if they are on systems that are often targeted by evil software.
2. Ensure antivirus is actually working: it's scanning for evil software and getting the latest updates.
3. Periodically check that it's working or, if possible, get notified when the antivirus software fails. Remedy failures quickly – especially if the failures affect critical or sensitive assets.

If you have a very large number of assets and need to focus your efforts, pay more attention to the critical and sensitive assets that you identified in the order that you ranked them.

Security Measures Against Vulnerabilities

The cost of neglecting vulnerability patching can result in IT troubles that are far more costly. Anyone from the outside can exploit vulnerabilities on externally facing assets to gain control of the asset. Compromised assets are used as a launch point to attack assets deeper in your IT infrastructure.

Patching software vulnerabilities soon after your software maker releases patches will better protect your systems. Apply patches as quickly as possible to minimize the duration the vulnerability is exposed.

Ideally, your security measures should do the following:

1. Keep up with vulnerabilities and patch releases for your software – especially on assets that are exposed to external people. Get your software maker to push that information to you.
2. Read the documentation so that you know the patch works on your particular asset configuration. Installing the patch on an identical non-production system and verifying that it doesn't cause problems reduces the probability of the patch breaking your assets.
3. Install the patch.

Assets with vulnerabilities exposed to external people should be your highest priority for vulnerability patching. The prioritization of patching other assets is driven by a few factors: the level of criticality and sensitivity of the assets, the severity of the vulnerabilities, and the size of the internal population who can potentially exploit the vulnerabilities from inside. The greater the number of internal people can exploit the vulnerability, the more urgent the patching is.

Products are available that can support the installation of patches to a large number of assets. Ideally the products should help you:

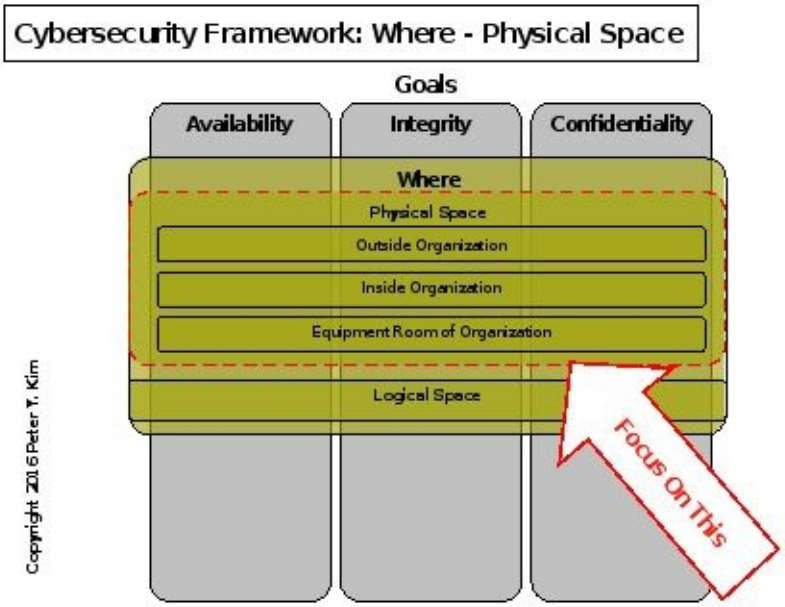
1. Provide visibility that patches are being successfully applied in appropriate priority.
2. Provide notification when the patching fails. Your IT should remedy failures quickly – especially if the failures affect external assets.

Conclusion

Use of antivirus and vulnerability management are two security measures that safeguard availability, integrity, and confidentiality. These measures should be considered a regular component of your IT security program.

Lesson 13: Security Measures for Physical Space of Cybersecurity Framework

Focus of This Lesson



Introduction

A variety of “bad things” can happen in the physical space to harm availability, integrity, and confidentiality. For example, someone can steal a traveling CFO’s laptop. A USB key containing confidential information can be stolen from someone’s cubicle. Someone can spill coffee on your core router in the equipment room and break it. Someone can plug cables into the wrong NIC unintentionally. People can do many things intentionally and unintentionally to undermine your security goals.

This lesson will focus on people caused events that undermine availability, integrity, and confidentiality in the physical space. It structures the discussion by looking at physical types of assets including portable media/storage devices, portable computers, desktop computers, and IT equipment.

This lesson will NOT cover physical hardware failures or failures caused by shortage of resources such as shortage of network bandwidth, memory/disk space or CPU time. Sizing assets appropriately, designing redundancy into your assets and having a tested process for recovery prevent these failures.

Essentially, physical security measures boil down to:

1. Encouraging people to physically protect assets from theft
2. Implementing physical barriers with doors and locks
3. Using processes to only allow the right people into the right places

Portable Media/Storage Devices - Anywhere

Mishandling of portable media and storage devices can lead to compromises in *confidentiality*. If a thief steals media or a device that happens to contain usernames and passwords, the thief can gain logical access to your resources and later undermine *availability* and *integrity*.

Portable media and storage devices containing sensitive information are sensitive assets that must be safeguarded. Security measures require encouraging people to keep/use them in a manner that reduces likelihood of "bad things" happening.

Habits To Encourage For Portable Media/Storage Devices In Any Physical Space

1. Do not keep sensitive information - especially unobfuscated usernames and passwords - on them unless you absolutely must.
2. If you must keep sensitive information on them, protect them against theft or loss. Treat them like you would with your wallet or purse.
3. Report theft or loss to your organization's authorities immediately.
4. If you use media like USB keys or other portable media to transfer data, then make it a habit to delete files on the media after each transfer. People copying data from your USB key to their computer can copy other files that were not meant for them. Be especially careful when you are transferring files to someone outside your organization like a client or a partner.

There are additional measures that can be taken. For instance, there are products that encrypt data on media to protect sensitive information. Encryption of data is helpful if the media contains sensitive data *and* is stolen. An organization that effectively exercises the above habits may be able to sufficiently reduce the probability of data theft without additional measures.

If the large majority of your organization does not handle sensitive data and effectively adopts the above habits, then an organization wide roll out of additional measures is probably not worth the cost. On the opposite extreme, if the large majority of your organization does handle very sensitive information, needs to store sensitive data in portable media, and doesn't adopt the above habits, then additional measures may be worth considering.

Backup Storage Media

Backup storage media require special attention because mismanagement of backup media can impact *availability*, *integrity*, and *confidentiality*. The theft of backup media undermines *availability* by undermining data recovery and also undermines *confidentiality* if the backup data is sensitive. Backup data can be altered to undermine *integrity* especially if the data is used for auditing or to restore production data.

Security Measures for Backup Storage Media

1. Store backup data in a separate location from your equipment room. If you keep backups in your equipment room and the room suffers physical damage from fire, flood, or a person, then your backups can be damaged together with the production equipment that rely on the backup data.
2. Protect your backup storage like you would your valuables. Keep them locked up. Allow only the right people to have access to them.
3. Report theft to your organization's proper authorities immediately.
4. If you do lose username and password data, ask everyone potentially affected to change their passwords.

There are additional measures that can be taken such as encryption. Again, if your organization follows the suggested rules of thumb, your security measures may be sufficient to secure backup storage media. Weighing benefits and cost of your security measures is a good idea.

Computers Outside and Inside Organization

Computers outside and inside your organization are subject to theft just like portable media and storage devices. Stolen computers differ from stolen media because a determined thief can potentially acquire logical access to resources that the computer has depending on how the computer has been configured.

For example, people often have their browser memorize usernames and passwords to web applications they frequently access. A determined thief can use those usernames and password. The thief who has logical access to resources can undermine *availability*, *integrity*, and *confidentiality* of your critical and sensitive assets.

Fortunately, stolen/missing computers do not go unnoticed for very long by their owners. Efforts to address theft/loss can be taken quickly.

The best way to reduce theft outside and resulting impact is to encourage your organization to adopt the following habits.

Outside: Habits To Encourage For Portable Computers

1. Prevent the theft of computers outside by treating your portable computers like your other valuables.
2. Report theft to your organization's authorities immediately. Quick reporting gives IT more time to react to the theft and less time to the thief to use the stolen computer to gain access to other resources.
3. If you do lose username and password data, change all potentially affected passwords immediately.

Computers inside the organization are best protected with a physical security measure and careful habits.

Inside: Physical Security Measure

Have a door lock / key system to guard against non-employees entering your office.

Inside: Habits To Encourage For Portable Computers

1. Keep your portable computer with you as much as possible. Take it home over weekends and overnight. Portable computers are easy to take out the door and susceptible to opportunistic theft.
2. Report theft to your organization's proper authorities immediately. Quick reporting gives IT more time to react to the theft and less time to the thief to use the stolen computer to gain access to other resources.
3. If you do lose username and password data, change all potentially affected passwords immediately.

It's hard to imagine people walking out the door with desktop computers, but it can happen. If you think you are particularly vulnerable, you may want to consider additional physical

measures that discourage theft of large items.

Additional Security Measures to Consider for Large Computers Inside Organization

1. Lock it down if a particular desktop can be used to gain logical access to sensitive/critical resources.
2. Monitor exit points of your office with cameras/people.
3. Require someone to sign out any large packages leaving the office.

The benefit and cost of security measures should be weighed before implementation.

Equipment in Equipment Room

Security measures for computers and network equipment in the equipment room follow a similar pattern as the others. Allowing the wrong guy to enter the equipment room can undermine *availability* because he can break things. Furthermore, as with personal computers, getting physical access opens more opportunity to gain logical access. Someone can plug into a box's serial port to gain logical access or add snooping equipment that can help that person gather sensitive information. When someone gets unauthorized logical access to critical assets, he can damage *availability*, *integrity*, and *confidentiality*.

Security Measures for Equipment Room

1. Have a door lock / key system to allow only authorized personnel inside the equipment room.
2. Don't enter the room with drinks or anything that can cause damage to equipment. It is not difficult to be careful and accidents do happen.
3. When making physical changes to the equipment, plan the change so you know what you are doing. An orderly equipment room and documentation that explains the stuff inside the equipment room can help you avoid cabling mix ups that can hurt the availability of your assets.

If your organization is doing a good job practicing the above security measures, you may deem those security measures sufficient. Implementing the above security measures may be easy for a small company but if you have a large company, then it may be harder for you to track who has the keys to enter the equipment room and who's actually going in and what's actually being performed.

Alternative Security Measures to Consider for Equipment Room

You might want to consider the following measures as an alternative.

1. Allow only a few key personnel to have a copy of the key to the equipment room. The key should not be easily copied. For the sake of this example let's say Joe and Tom have the only two keys.
2. When someone – say Jennifer - must go into the equipment room, then Jennifer must request the key to the equipment room from either Joe or Tom. She goes to Tom.
3. Jennifer must explain to Tom what she needs to get done in the equipment room. Tom approves. Jennifer and Tom sign a document that verifies Tom has given the key to Jennifer.
4. Jennifer must return the key to Tom before the end of the day or when she completes the task. This is both Tom and Jennifer's responsibility. Jennifer and Tom sign a document that verifies that Tom now has the key.

The above security measure was presented to show that implementing a process can increase security; you don't need buy high tech solutions to enhance security. It's also important to note that each security measure can have its "challenges." In this case, either Joe or Tom must always be accessible to Jennifer just in case there's an emergency and Jennifer must enter the equipment room immediately.

Conclusion

Although this lesson is a presentation of common sense measures, there are a few points worth noting.

Security measures can be lots of things other than technology:

1. Influencing people's behavior
2. Making physical barriers
3. Using processes

There isn't one way to implement physical security measures. The general goal of physical security measures is to allow physical access only to the right people. There are lots of ways to implement measures to satisfy the goal and each method has varying strengths and weaknesses.

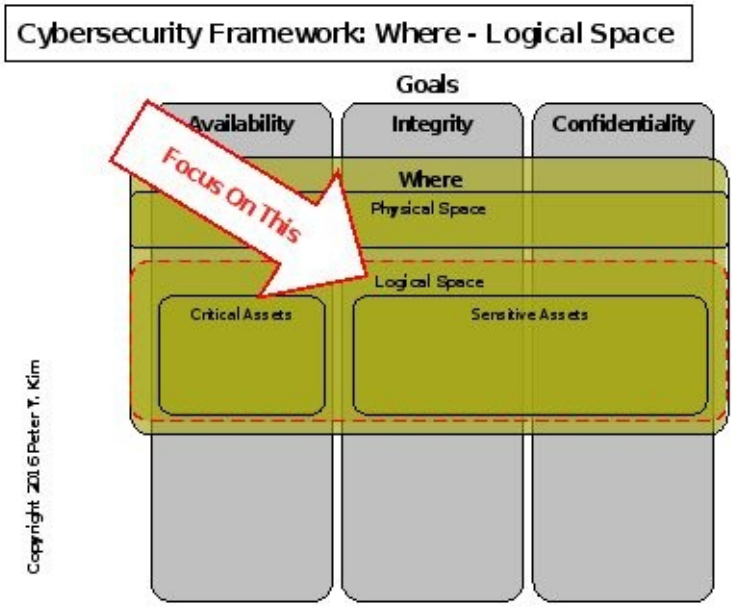
The better job you do of implementing "upstream" security measures, the less important "downstream" security measures are. For example, if you do a great job with only allowing the minimum number of "right" people to have access to the equipment room, you don't have to worry about monitoring the actual activities in the equipment room with a camera. If you aren't sure who all have the keys to the equipment room, then you might want to consider additional measures such as camera monitoring to discourage unauthorized personnel from entering.

Cost of security measures not only includes the money spent on locks and cameras, but time and energy spent exercising the process or the negative impact on user experience. For instance, encrypting PC hard drives can slow things down and hurt user experience.

Lastly, the benefit and cost of security measures must be assessed by each organization and each may choose different or more stringent measures that fit its unique needs.

Lesson 14: Routes in Logical Space to Compromise of Availability, Integrity, Confidentiality

Focus of this Lesson



Introduction

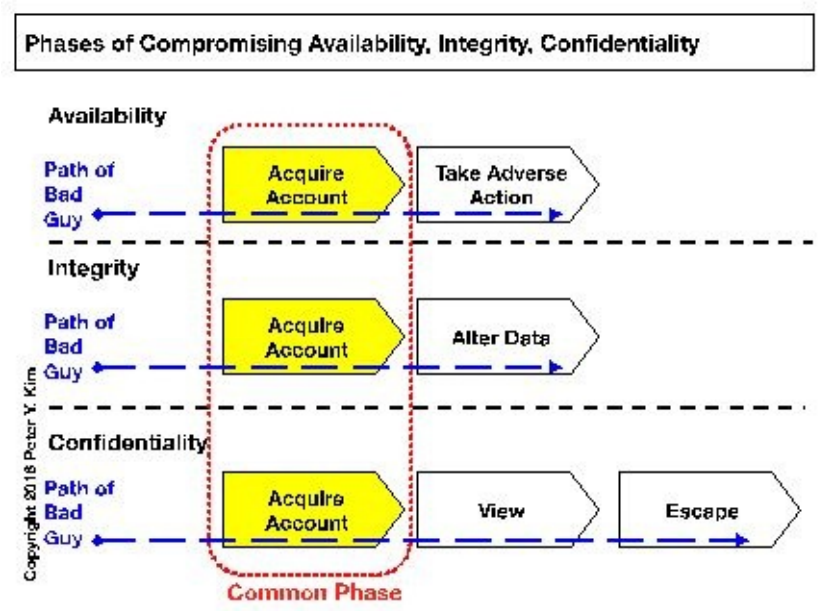
Previous lessons covered the types of security measures, security measures against “What” and physical space components of the Cybersecurity Framework. This lesson will focus on the logical space.

The route for someone to compromise availability, integrity, or confidentiality, has recognizable phases.

Phases to Compromise of Availability, Integrity, and Confidentiality

An external hacker can exploit vulnerabilities in externally facing software to compromise availability, integrity, and confidentiality. For instance, vulnerabilities in externally facing web applications can be exploited to alter or steal data, or even damage the operation of the computer. These damages can be inflicted without acquiring an administrative account on any application or software. However, acquiring an administrative account allows far greater access to data and IT operations; therefore, acquiring an account is of strong interest to "bad people."

The route to compromising availability, integrity, and confidentiality starts with acquiring accounts on assets.



Availability

1. Someone gains control of an account on a critical asset.
2. He can then take a variety of actions that can undermine the availability of your critical assets. For instance, he can shutdown a host or reconfigure an asset to be inaccessible to everyone else. He can delete critical data.

Integrity

1. Someone gains control of an account on a sensitive asset.
2. He can then alter sensitive data. For instance, he can add false sales records so that the organization's financials are overstated or give himself a raise in the payroll database.

Confidentiality

1. Someone gains control of an account on a sensitive asset.
2. He can view data.
3. He can “escape” with the sensitive data.

Security measures that protect against unauthorized acquisition of accounts are very important in preventing bad things from starting.

We assumed that one person was going through these phases. There can be multiple people involved in the compromise of data confidentiality. Someone may have access to sensitive data that he shares with someone. The second person can then escape with the data.

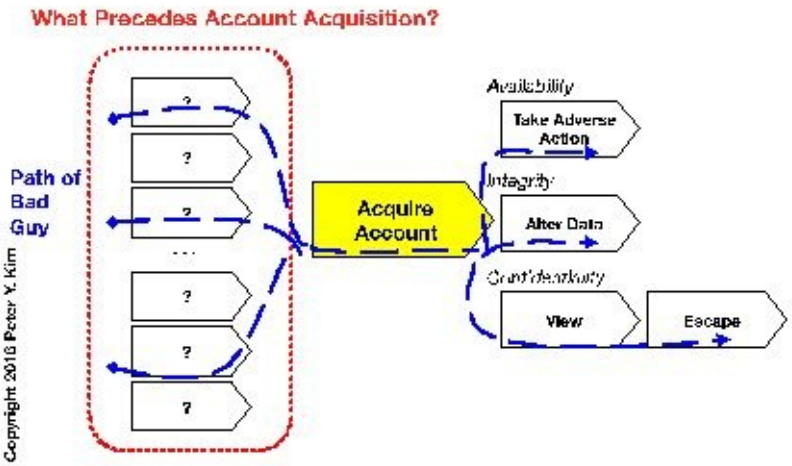
Conclusion

Acquiring control over accounts is a step toward undermining availability, integrity, and confidentiality. The following lesson will discuss routes users can take to acquire accounts.

Lesson 15: Routes to Acquiring Accounts – External Users and Security Measures

Focus of This Lesson

Phases of Compromising Availability, Integrity, Confidentiality

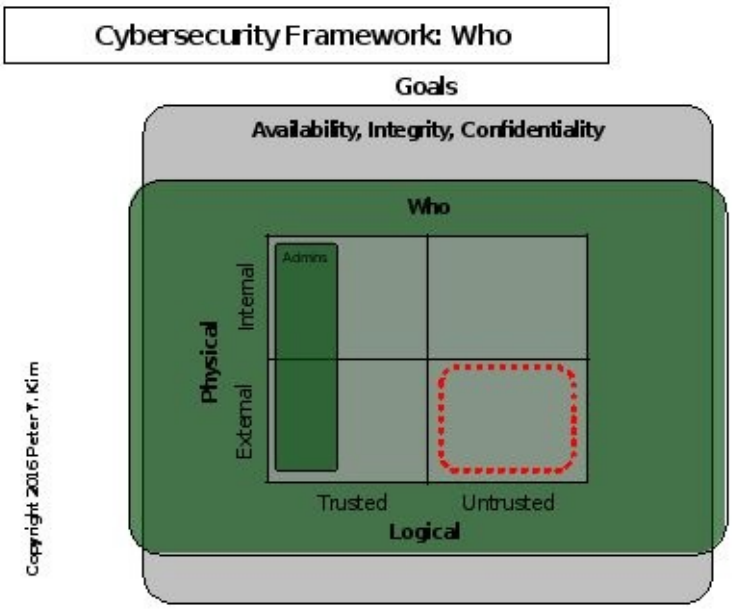


Introduction

A previous lesson defined phases to compromising availability, integrity, and confidentiality and identified “acquire accounts” as a common phase. Understanding how someone can unrightfully acquire accounts can help us create security measures to prevent it.

This lesson organizes the discussion by different groups in the “Who” of the Cybersecurity Framework. This lesson will discuss external trusted and external untrusted users.

Who: External Untrusted



Someone can gain control of an account by hijacking someone else's account or getting one created.

Context For Discussion

Let's imagine an organization that runs an online web trading service. The organization's customers use web screens to trade stock in real time. An untrusted user is someone who does not have a trading account. A trusted user is someone who does.

The web server and related network equipment only allow connections to http and https. No other ports are open. The application is designed to only allow the display of the login screen to anyone who has not authenticated.

This lesson will list examples of ways that an external untrusted person can gain access to a trading account or an account of the operating system that the web application runs on. Security measures are suggested.

Example 1

Acquisition Route: Steal usernames and passwords by eavesdropping network packets.

Security Measure: Design – Encrypt transmissions of usernames and passwords.

Example 2

Acquisition Route: Guess usernames and passwords – use brute force.

Security Measures:

1. Design – Only allow use of strong passwords.
2. Monitor - Upon three consecutive failures to login, lock the account so no more attempts can be made. Notify administrator that there have been three failed attempts.

Network equipment often have default usernames and passwords. Delete these commonly known usernames and passwords from equipment.

Example 3

Acquisition Route: Exploit vulnerabilities of an unwary trusted user's web browser to acquire trusted user information. Use that information to take over trusted user's account.

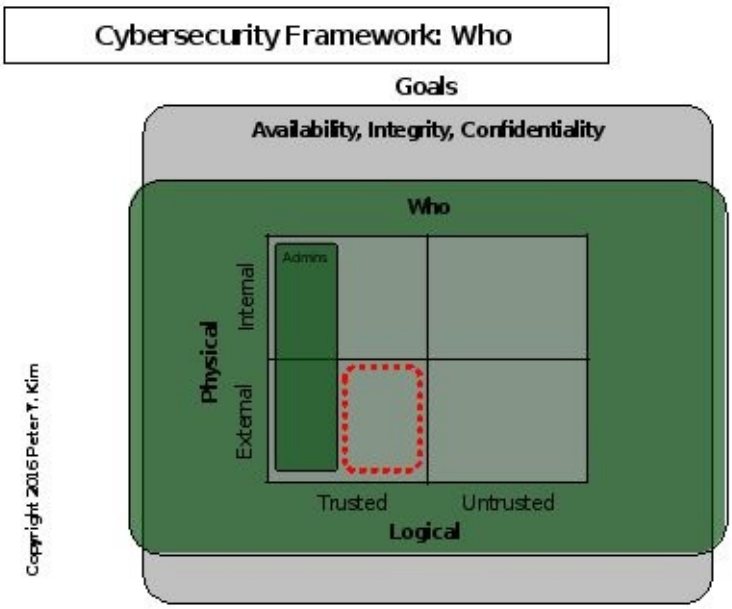
Security Measure: Design – When someone logs in from an IP address that has never been used to log into an account, then ask user self-identifying information to verify identity following successful login with username and password. Self-identifying information can be mother's maiden name.

Example 4

Acquisition Route: Exploit vulnerabilities in web application, web server, operating system to gain control of the host.

Security Measure: Maintain - Patch vulnerabilities as quickly as possible.

Who: External Trusted



Let's continue using the web trading context to go through examples of external trusted users.

Trusted users already have a username and password and are given access to web application screens that are not accessible to untrusted users. Trusted users can attempt to do harm to your asset by exploiting vulnerabilities in your web application. Trusted users have the option of using routes that are available to external untrusted users.

Acquisition Route: Exploit vulnerabilities in web application.

Security Measures:

1. Design – Make your web application validate all parameters passed to the web application so that values are what you expect. Guard against insertion of code into text.
2. Monitor – Make web application notify your security team when user attempts to enter harmful text.
3. Monitor – Make web application notify your security team when user tries to access a page that he doesn't have permission to access.

Upon Acquiring an Account

An external untrusted user who hijacks accounts on the web application can place trades without the knowledge of the real account owner. An external untrusted user who gains administrative control of the operating system of an asset can take a variety of actions to cause damage. Furthermore, he may use the compromised asset as a launch point for penetrating deeper into your IT infrastructure.

Reaction Plan

Once the compromise of an asset is detected, you must decide how to react. Do you want to lead him to believe that he's undiscovered and monitor him to accumulate evidence against him to take to court?

It can be very difficult to identify all the changes an intruder made to your computing resources and reverse them. Once you understand how he penetrated your asset, do you want to take the computer offline and do a fresh reinstall with the vulnerability fixed? It's probably a good idea.

Do you want to notify the owners of the accounts that were broken into?

It's up to your organization to determine the reaction plan to the results of the compromise. Having a human organization ready to determine the next steps is important.

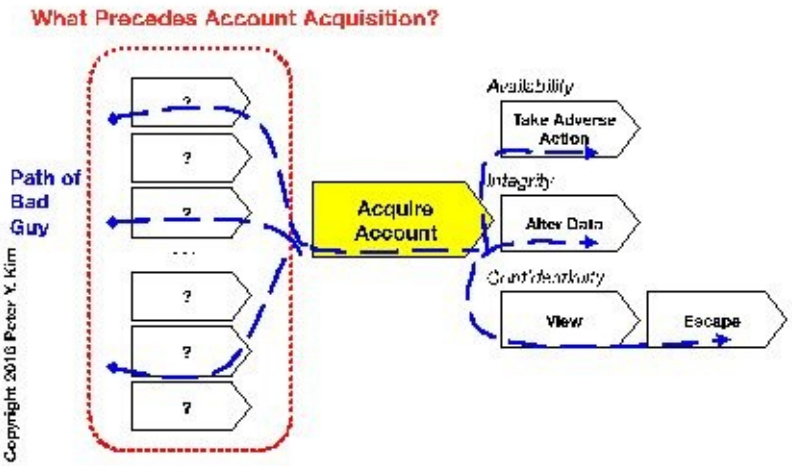
Conclusion

By understanding the routes that are available for external trusted users and external untrusted users, we can formulate security measures that block each route. A range of design, maintain/monitoring, and reaction plan measures were presented. The next lesson will cover internal untrusted and internal trusted users.

Lesson 16: Routes to Acquiring Accounts – Internal Users and Security Measures

Focus of This Lesson

Phases of Compromising Availability, Integrity, Confidentiality



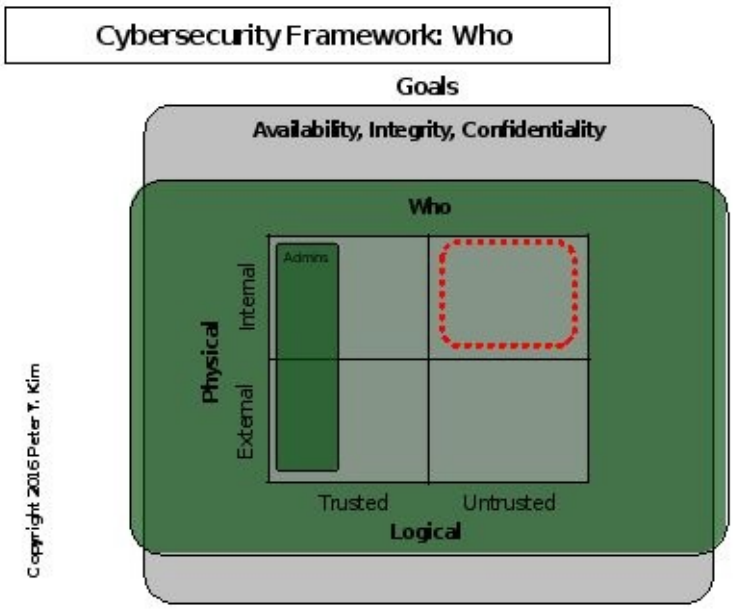
Introduction

This lesson continues the discussion started in the previous lesson; the previous lesson discussed routes that external untrusted and external trusted users could take to acquire accounts. This lesson discusses routes internal untrusted and trusted users can take.

External users are largely confined to using routes in the logical space to acquire access to externally facing assets. In contrast, internal users have access to a physical space that external users do not have; they reside in the office so they can physically access computers and influence people at the office. Therefore, internal users have a set of routes in addition to the routes available to external users. Internal users can attempt to acquire access through using external user's tactics like exploiting a vulnerability of an asset, but they are more likely to use the easier routes suggested below.

Many of the internal security measures require influencing the behavior of people.

Who: Internal Untrusted



Internal untrusted users can use exploit tactics to gain control of internal assets just like external users use against externally facing assets. For internal users, there are additional routes.

Context For Discussion

Let's imagine a public company. It must report its quarterly financial performance to its investors. Safeguarding the integrity of its accounting data is an IT requirement. The IT team must ensure that the right people enter the data.

Example 1

Acquisition Route: Ask for an account from IT.

Security Measure: Design – Make a process that checks that only the right people get accounts and the right people get right privileges.

Often, the person who is responsible for administrating a system does not know who should have accounts and what privileges they should have. The administrator may end up providing an account without asking any questions.

Making a process that makes the administrator verify that the requester should in fact be provisioned an account with the authority of the asset is a possible security measure. This measure is more important the more critical or sensitive the asset is. The process need not be elaborate. In this case, the administrator would contact the authority in the accounting department to confirm that an account should be provided with what privileges.

Example 2

Acquisition Route: A coworker shares his username and password because you need temporary access or he needs your help.

Security Measures: Design – Discourage sharing of usernames and passwords no matter what the reason.

Users often use the same usernames and passwords across multiple assets because they don't want to memorize multiple passwords. Someone can share his password for an asset that is NOT sensitive, but the same password may allow access to assets that are far more sensitive. The person who receives the username and password pair can try to use them on other assets.

For example, someone can share his password for an internal portal; however, the password for the wiki may be the same as his accounting system account.

Example 3

Acquisition Route: Memorize a password that is written down on a piece of paper in open view in someone's cubicle.

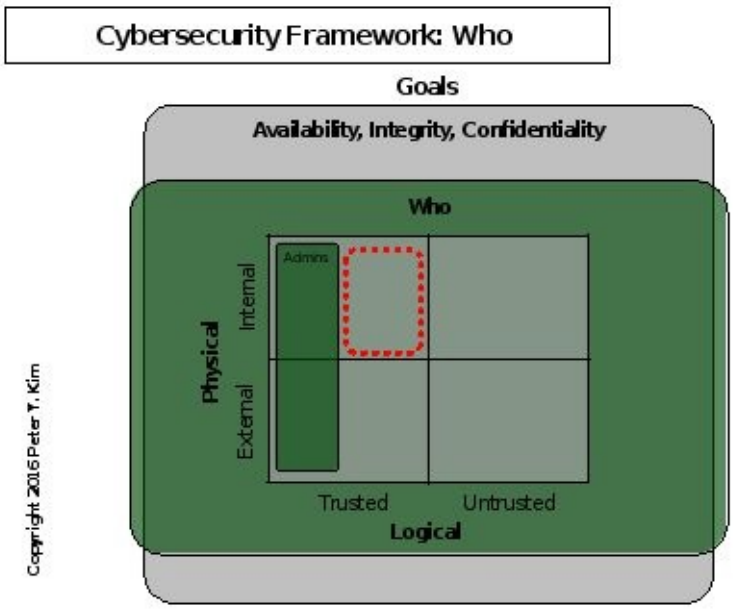
Security Measure: Design – Encourage behavior that conceals passwords.

Example 4

Acquisition Route: Memorize a password that is being typed in open view.

Security Measure: Design – Encourage behavior that conceals passwords.

Who: Internal Trusted



Internal trusted users have the option of taking the same tactics as an external user. They can try to exploit vulnerabilities that are exposed to gain administrative control over an asset.

Internal trusted users can explore the data that is already available to them. Some assets contain files with usernames and passwords that may be discovered by a trusted user if the administrator does not take proper precautions. For instance, Unix operating systems can have a /etc/passwd file that contains usernames and passwords.

Trusted users who find this data can use other people's accounts without the knowledge of the real account owners.

Acquisition Route: Steal usernames and passwords within asset. For example, the /etc/passwd file of Unix operating systems can be left open to the view of trusted users.

Security Measure: Design – Obfuscate or encrypt password data in all assets.

Upon Acquiring an Account

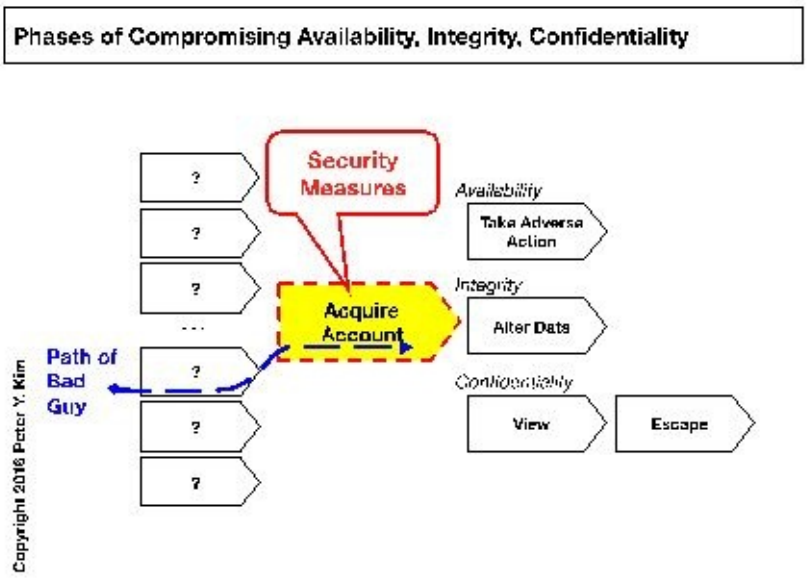
People with accounts can move to the next step in harming availability, integrity, and confidentiality. Some trusted users may pursue administrative access rights by exploiting vulnerabilities in the applications that they now have access to.

Conclusion

By understanding the routes that are available for internal users, we can create security measures that can block each route. The examples presented in this lesson were largely habits that the company should promote as company policy. The participation of each member of your organization is important to an effective security program.

Lesson 17: Security Measures for Accounts Management

Focus of this Lesson



Introduction

Even with disciplined implementation of the security measures that block unauthorized acquisition of accounts and privileges, your IT team should consider implementing maintain/monitor measures as a second line of defense.

The following examples will help you get a feel for what to maintain and monitor. They are largely measures that "keep your ducks in a row." The difficulty of implementing the security measures depends on the assets you are safeguarding. Some applications may already generate reports that support these measures.

Security Measures

These measures require the collaborative effort of system administrators and the "authorities" of the assets. For example, an administrator of an accounting application must work together with the accounting department's authority to agree on which accounts to delete. An administrator of an operating system may need to confirm with his manager about deleting accounts from an operating system.

Accounts Management

1. Delete needless accounts. If George Washington left the company, delete his accounts. Someone can continue using George's accounts without the knowledge of the proper authorities. Delete unused service accounts.
2. Delete dormant accounts. Abraham Lincoln is still with the company, but he hasn't used his account on the ABC Accounting Application for a long time. Why does he have it? If he doesn't need it anymore, delete it.
3. Make sure no new accounts are being made without knowledge of the proper authorities. If a new account "benjamin.franklin" is added but it does not map to a real person or it doesn't map to a service account, something fishy is going on.

Privilege Management

1. Make sure no accounts are being placed in a group without the knowledge of the proper authorities. Adding accounts to groups can give the account the privileges attached to the groups.
2. Make sure no single account is expanding its privileges (e.g. creating accounts) without knowledge of proper authorities.

Group Management

1. Delete empty groups. If nobody is in a group, why is it there? Delete it.
2. Make sure no new groups are being created without knowledge of proper authorities.
3. Make sure no group is acquiring privileges without knowledge of proper authorities.

General Management

1. Make sure that administrative actions are performed by the right users. If a user behaves like an administrator but is not one, something fishy is going on.
2. Make sure that no new trust relationships are being created without knowledge of the proper authorities.

Implementation of Measures – Illustrative Examples

The difficulty of implementation will vary with the asset. The asset might already have built-in capabilities that generate the reports described below. An enterprise wide roll out that implements the security measures for all assets is not necessary. You can focus only on critical and sensitive assets.

This section proposes an implementation approach for an accounting system fictitiously named “Accounting Pro” of a medium-size business of a few hundred to a few thousand people.

For the purpose of explaining these examples, let’s assume that reports that support the above security measures are generated periodically once a quarter. Each time the reports are generated, they cover a period of time between now and the previous time the reports were generated.

Because you are generating reports for a particular asset and not the entirety of the enterprise, the reports will contain a manageable number of records. It is hard to imagine an accounting team of a hundred people for even a company with a few thousand employees.

The following set of reports can help the head of accounting, the person in charge over the use of the system, determine if the right people have accounts and support the security measures described above.

Reports Examples

1. All User Accounts – A snapshot view of all accounts. If there are 20 people total in the accounting department, it may be worth figuring out why there are 5 extra.

All User Accounts On Accounting Pro

On: 11/30/2016

Total # of User Accounts: 25

#	Username	Name
1	abraham	Abraham Lincoln
2	george	George Washington
3	tom	Thomas Jefferson
…		

2. Added User Accounts - List of users that were added during period. You can see if someone who wasn't supposed to be added, was added. You can detect this problem on the All Users report but it's more easily detected on this report.

User Accounts ADDED On Accounting Pro

Period: 11/1/2016-11/30/2016

Total # of User Accounts ADDED: 5

#	Username	Name
1	abraham	Abraham Lincoln
2	george	George Washington
3	tom	Thomas Jefferson
…		

3. Deleted User Accounts - List of users that were deleted during period. If someone left the company and he's not on the deleted list, there's a problem. You can detect the same problem on the "All Accounts" report, but it's easier to detect here.

User Accounts DELETED On Accounting Pro

Period: 11/1/2016-11/30/2016

Total # of User Accounts DELETED: 4

#	Username	Name
1	barack	Barack Obama
2	bill	Bill Clinton
3	ronald	Ronald Reagan
…		

4. Dormant Accounts - List of users that did not log into Accounting Pro during period. This helps you identify accounts that should be deleted.

User Accounts DORMANT On Accounting Pro

Period: 11/1/2016-11/30/2016

Total # of User Accounts DORMANT: 3

#	Username	Name
1	herbert	Herbert Hoover
2	jimmy	Jimmy Carter
3	teddy	Teddy Roosevelt
…		

Similar reports can be made for the other security measures for privilege, group, and general management.

We assumed that the above reports were generated quarterly; however, you may want to generate them more frequently in order to catch “fishy” things as quickly as possible.

Here’s another approach. The reports are generated daily; however, if there are no additions or deletions to accounts, then IT security team is notified that nothing has changed. This helps the IT Security team avoid spending time with non-informative reports.

Approaches to Generating The Reports

If your application cannot generate these reports, then there may be other roundabout ways to generate them.

Your application may generate a log that keeps track of account additions and deletions. Not all applications can do this. If it does, then you can parse the log file to create the “all,” “add,” and “delete” reports. You can develop this, find a freely available program, or buy a product that can help you.

If your application can only generate a list of usernames, then you can identify the differences, additions and deletions, and generate the report. It is important to note, however, that this method of generation will miss accounts that were added and deleted in the same period.

Your application may generate a log that records which accounts were logged into when. Not all applications can do this. If your application can do this, you can parse the log file and reference a list of all existing user accounts to roughly determine which accounts were dormant.

Going Beyond the Example Reports

There are plenty of other reports that may be possible. For instance, if you noticed that user accounts were being mysteriously added, then you would want to know who added it. Generating the “add” report with the username of the administrator might be helpful in this case. You may choose to generate this report as part of the quarterly routine or request an investigation by the IT team if the need arises.

Again, the feasibility of making this report relies on the capabilities of your application. If no such data is kept in your application, then generating the report will be very difficult.

Security Measures for the User

So far, we've discussed what the system administrator and the head of accounting could do to safeguard against unauthorized account acquisition. There are security measures that individual users of the system can follow to protect their account against hijacking.

For any Saas software that requires login, configure the software to send an email to the user upon login so that the account owner knows that someone else has logged into his account. The owner can notify the proper authorities.

If the application displays the previous time the account was active when the user logs in, the user can check whether he was actually the guy who last logged in. If he logged in two weeks ago but the last login record shows his last login as yesterday, something fishy is going on.

Encouraging your users to check the last login dates every time he logs in and to report anything fishy to the proper authorities can enhance your security.

Reaction Plan

If something fishy is detected with the above measures, then you should investigate the root cause. Depending on the results of the investigation, you may want to take disciplinary action or implement more security measures if you discover a weakness in your measures.

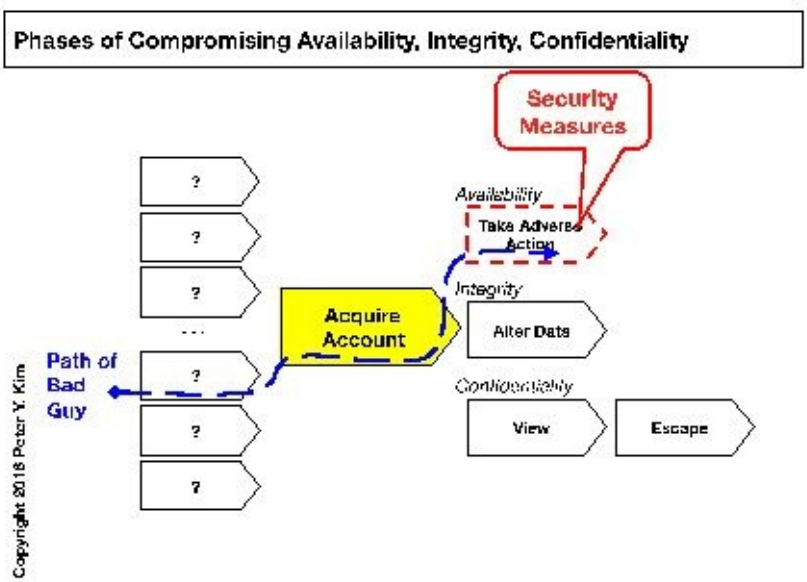
Conclusion

This lesson presented ideas on maintaining and monitoring accounts in an accounting system as a measure to make sure that wrong people do not have accounts. Using an old account of someone who has left the company is a security hole that people can take advantage of. Keeping “your ducks in a row” is an important practice that organization should adopt to reduce the probability of compromises to availability, integrity, and confidentiality.

It is important to point out that, in general, one account should only be used by one person and never shared. This eases mapping of accounts to their rightful owners. When accounts are shared, then tracking who did what becomes very difficult.

Lesson 18: Security Measures for Availability

Focus of This Lesson



Introduction

In addition to the security measures preventing unauthorized account acquisitions, another layer of security measures can be applied downstream in the logical space for critical assets. Costs and benefits of these downstream security measures should be considered before their implementation. The more effectively upstream measures are implemented, the less valuable downstream measures may be.

These measures can also be considered when you are concerned about trusted administrative users going “rogue” and inflicting harm against your organization.

Security Measures

Security measures that safeguard availability detect unauthorized changes to the configuration of critical assets. Unauthorized changes can change the expected behavior of computers and network equipment, and undermine their availability.

1. Prevent unauthorized changes to high availability configurations
2. Prevent unauthorized changes to network equipment such as firewalls
3. Prevent unauthorized changes to backup mechanisms

Once critical assets are correctly configured for high availability, security measures can be taken to protect against unauthorized changes to their configurations. Unauthorized changes can render the high availability mechanism inoperative.

The configuration of network equipment is changed infrequently after it has been put into production. Again, the correct configuration of the equipment must be protected against unauthorized change.

Changes to the configuration of backup mechanisms of critical assets must be protected for the same reasons. An operative backup mechanism must be protected from unauthorized changes that can undermine the availability of critical data.

Implementation of Measures – Illustrative Examples

The difficulty of implementation will vary with the asset.

This section proposes an implementation approach can apply to any organization.

Someone with an unrightfully acquired account must log on before he can make any configuration changes. The frequency of logins should be very low and the configuration should only change as part of intended maintenance. Therefore unusual logins and changes to configuration files can be an indicator of “bad things” happening.

Please remember that these security measures that apply after someone has already acquired an account.

Instead of periodic reports, real-time alerts may be more appropriate because harm that can be done can be catastrophic.

Alert Examples

1. An alert should be sent to the IT security team when someone logs into any account on network equipment – equipment that should not be frequently changed.

Alert – Firewall Successful Login

Firewall IP Address: 67.233.79.10

User Account: xjdSa1f0KQ

Login Time: 11/1/2016 13:01:26 PST

Login from IP Address: 192.168.0.34

Please confirm that this login is for scheduled maintenance work.

2. An alert should be sent when the configuration of network equipment, high availability mechanism, or backups has been modified.

Alert – Firewall Configuration Has Changed

Firewall IP Address: 67.233.79.10

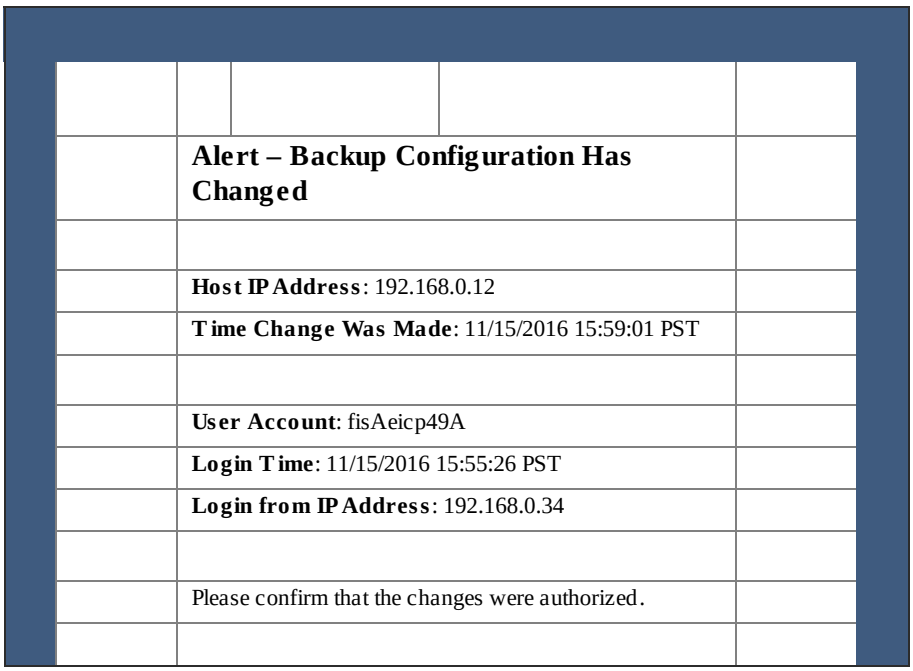
Time Change Was Made: 11/23/2016 10:42:42 PST

User Account: xjdSa1f0KQ

Login Time: 11/23/2016 09:15:18 PST

Login from IP Address: 192.168.0.34

Please confirm that the changes were authorized.



In order to identify the changes made, you should make it a habit to save the configuration in a protected location apart from the equipment. The current configuration file can be diff-ed with the latest copy of the configuration file that you saved to identify changes. Saving your configuration files will also allow you to reverse changes. There are products that can help you with management.

We have been assuming rogue users making adverse changes. However, sometimes legitimate users make mistakes that harm availability. Saving configuration files of your critical assets can help you recover from legitimate mistakes.

Going Beyond the Example Alerts

Another approach to identify unwanted logons or configuration changes would be set time windows for which maintenance is typically done. If logons or changes occur outside this time block, then an alert can be sent.

You should not limit yourself to the presented alerts if you feel there are other alerts that better fits the needs of your organization.

Security Measure - Monitor Backups

Backups can fail for reasons other than adverse changes to its configuration. Therefore, it is important to monitor that backups are being successfully taken. An alert should be generated for each successful and failed backup. An alert for a successful backup verifies that the backups are indeed being taken. The failure of the backup warrants immediate response.

Reaction Plan

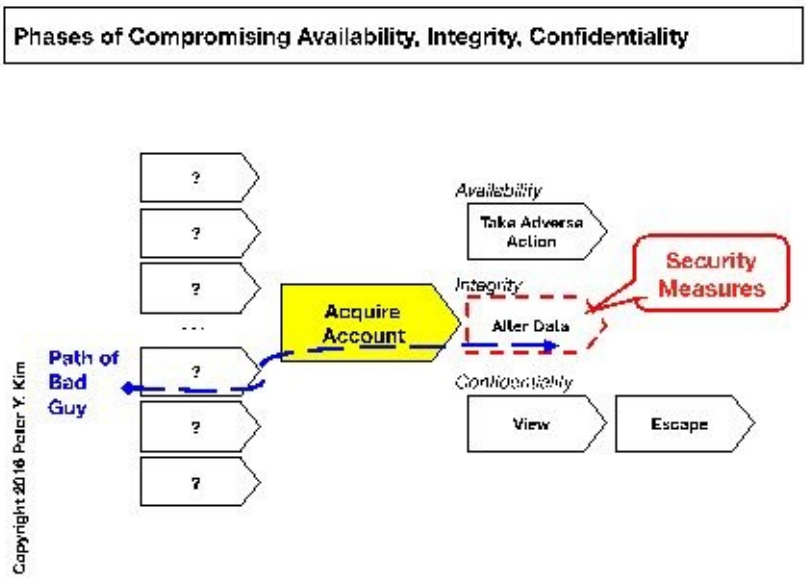
If something fishy is detected with the above measures, then you should investigate the root cause. You should decide your next steps depending on the results of the investigation.

Conclusion

We covered additional measures that can be taken as lines of defense in addition to the initial safeguards of providing accounts and appropriate privileges to the right people. These measures can also help you detect a rogue administrator who is undermining the availability of your critical assets.

Lesson 19: Security Measures for Integrity

Focus of This Lesson



Introduction

In addition to the security measures preventing unauthorized account acquisitions, another layer of security measures can be applied downstream in the logical space to safeguard integrity. Costs and benefits of these downstream security measures should be considered before their implementation. The more effectively upstream measures are implemented, the less valuable downstream measures may be.

These measures can also be considered when you are concerned about trusted users going "rogue" and inflicting harm against your organization.

This lesson follows the pattern established by the previous lesson about safeguarding availability. The additional layer of security measures involves tracking the changes to data and who made the changes.

Data Access Points

There are multiple logical access points to data. Someone can access data through a client application. For instance, someone can use an account on an EMR system to retrieve patient records; the EMR client is an access point. However, if this data resides inside a database, then someone can directly access the data in the database with the database client instead of the EMR client.

It is important to use this idea when applying account management security measures discussed in an earlier lesson. The accounts of both the EMR system and the underlying database should be maintained.

Security Measures

There are two types of data worth distinguishing because the approaches to safeguarding their data integrity differ:

1. Data that should never be changed by anyone
2. Data that should be changed by the right people

Data That Should Never Change

Historical data should never be changed. Examples include financial accounting history, bill payments history, stock trading history, and patient history. When corrections need to be made, records that correct the history are added as new data. Nothing should be deleted or modified. Information about new transactions are added as new data.

The two security measures that can be taken to safeguard integrity of this data are:

1. Make sure that existing data is not being changed.
2. Make sure that new data is authorized.

Data That Should Change

The billing address of a utilities customer must be changed at the customer's request, so the monthly bill is delivered to the right address. Someone who's changing her name after marriage will report the change to her credit card companies.

The security measure for this data is similar to the second measure above:

1. Make sure that changes are authorized.

Implementation Approach – Illustrative Examples

The difficulty of implementation will vary with the asset. Some applications will already have mechanisms for reporting changes. Others might generate an audit log that captures change history. There are many approaches to implementing these measures; there is no single correct approach.

This section describes a hypothetical approach to implementing the measures on an electronic medical record system [EMR]. The point of the example is to illustrate a possible approach at a high level; I make big assumptions about the capabilities of the EMR system and make simplifying assumptions about the patient history data structure.

Data about a patient includes basic elements:

1. Content data – This includes data created by the doctor about the patient or test results.
2. Meta data – This includes data about the content: who entered the content, when and from where.

Data That Should Never Change

A message digest algorithm can be applied to historical data and the generated hash can be kept as a baseline. Periodic comparisons can verify that the hash of the historical data is the same as the baseline hash. If the hash changes from the baseline hash, there's something fishy going on and is worth generating a report that shows a "diff" comparison to identify the changes that were made. Ideally, a report would show what changes were made and show "before" and "after" versions of the data.

An alert should be sent whenever the data integrity check is completed. A successful integrity check will ensure that the checks are actually being done. Since changes to this data should never happen, an alert should be sent to the IT security team when they are detected.

This baseline hash should be regenerated whenever new data is added. Before the new data is added, the existing baseline hash should be compared with the hash generated with the old data to confirm that the old data has had no unauthorized changes.

The reaction plan can involve locking down the patient record so that the patient record is not used by an unwary doctor or nurse. Reverting the patient record to the original state and investigating the root cause of the data change will probably be additional steps.

New Data

New data should be added by only the right people. Security measures for account management covered in an earlier lesson address this.

Some additional measures can be considered as extra layers of defense. For instance, when someone submits an update to the patient record, he can be prompted for his password again so that each submission is tightly bound to the submitter. If a doctor leaves the EMR application session open without logging off, the wrong people can masquerade as a doctor and enter bad submissions. At the end of the day, the doctor can review a summary of documents that he added to his patients' files and verify that the right files have been added.

Data That Should Change

Data should be changed by only the right people. Security measures for account management covered in an earlier lesson address this.

If the patient's billing address has changed, then the person entering the change must verify that the person requesting the change is in fact the patient before changing the address. The "right" people, in this case, are the patient and the person entering the new address.

Trusted Users Abusing Accounts and Privileges

So far we assumed that people who unrightfully gained access were altering data. Additional security measures that monitor the activity of trusted users can be taken. You may have a rogue doctor or nurse adding false data. You should consider the cost of taking such measures – the cost of implementing the technology and the people time that must be used to support the measure.

Having doctors and nurses not only sign off on the submissions they make themselves but the submissions of their teammates can be a measure to detect a single rogue user who is entering incorrect data. That is, if a doctor and a nurse submitted new data for patient John Smith, then the doctor will check the nurse's submission and the nurse will review the doctor's.

A security measure to guard against rogue trusted users collaborating to falsify data is to have someone apart from the people who entered the data independently review the data. This person must have the expertise to detect that something is wrong. Again, the cost and benefits of implementing this kind of measure must be considered.

Going Beyond the Examples

The core principles of checking data integrity do not change and can be applied to everything from file systems to databases. The above measures help you understand the general principles. Your implementation will vary depending on the capabilities of your system.

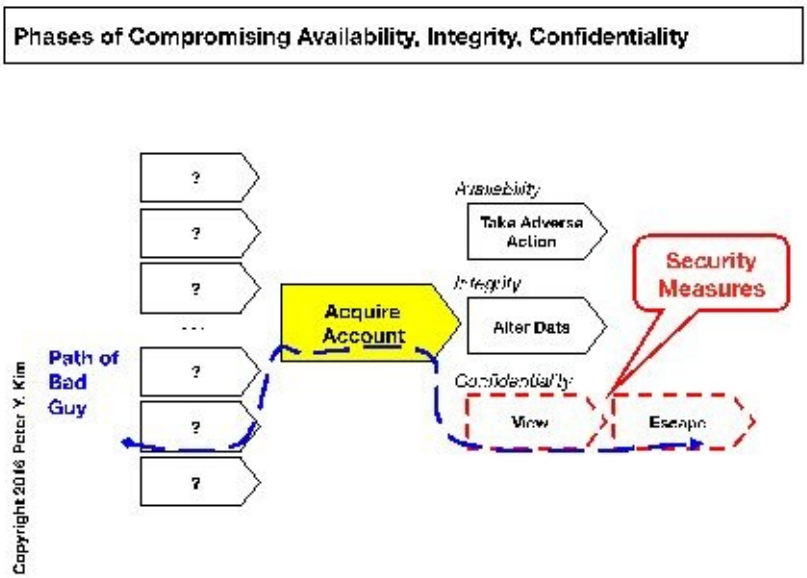
For instance, an accounting system contains historical data that should not be modified; new data is entered by only the accounting team. Again, the above approach can be used to verify that already entered data is not being changed. Furthermore, making sure that the right person is entering the new account entries will better ensure that bad data is not being entered. A periodic internal audit process that has the head of accounting inspect all newly entered data can ensure that the right data is being entered.

Conclusion

We covered additional measures that can be taken as lines of defense in addition to the initial safeguards of providing accounts and privileges to the right people to protect data integrity. These measures can also detect trusted users gone rogue.

Lesson 20: Security Measures for Confidentiality

Focus of This Lesson



Introduction

In addition to the security measures preventing unauthorized account acquisitions, another layer of security measures can be applied downstream in the logical space to safeguard confidentiality. Costs and benefits of these downstream security measures should be considered before their implementation. The more effectively upstream measures are implemented, the less valuable downstream measures may be.

These measures can also be considered when you are concerned about trusted users going "rogue" and inflicting harm against your organization.

This lesson follows the pattern established by previous lessons about safeguarding availability and integrity. The additional layer of security measures involves monitoring the actual viewing activities of the user and monitoring/blocking the information from escape.

Data Access Points

There are multiple logical access points to data. Someone can access data through a client application. For instance, someone can use a sales management system to view customers' purchase histories and their credit card numbers. The software client to the system's application is an access point. However, if this data resides inside a database, then someone can directly access the data in the database without the software client.

It is important to use this idea when applying account management security measures discussed in an earlier lesson. The accounts of both the application and the underlying database should be maintained.

Security Measures

Security measures in addition to the account management measures described in an earlier lesson can be considered for preserving data confidentiality.

One security measure is to track which trusted user is viewing what information.

The thief must escape with sensitive data beyond the boundaries of your IT infrastructure to profit. Blocking the thief's escape is another measure that can be taken to safeguard data confidentiality. The escape routes are numerous and some are extremely difficult to block.

Escape Routes of Sensitive Information:

1. Memorize it.
2. Write it down.
3. Print it out.
4. Send it via facsimile.
5. Copy and paste it into a web mail service – if not text, then take screen captures and upload as attachment to web mail service.
6. Send it out as attachment in email from company account.
7. Send it out as body of message in email from company account.
8. Transfer the file using FTP, scp, or similar file transfer client.
9. Transfer using peer-to-peer file sharing clients or applications like Skype that support file transfer.
10. Transfer data to portable media like a USB memory key or other portable storage device, and leave with device.
11. Transfer data to writable DVD's or CD's and leave with media.

Security measures that safeguard confidentiality are:

1. Monitor who is viewing sensitive information.
2. Block escape routes.

Implementation Approach – Illustrative Examples

Let's assume that we are an e-commerce company that stores customer credit card information. A web application calls the credit card numbers so it can place a charge on the customer's credit card when he checks out his shopping cart. We are safeguarding the confidentiality of credit card numbers.

Monitoring Who Is Viewing Sensitive Information

Application logs or database logs are potential sources of information to monitor which users are viewing what. However, logs may not generate the information that you need to implement the security measures. If the logs do generate the information that you need, the logs will generate other information that you do not need. You may collect so much data that no analysis tool can easily process the records that you need.

If logs do not contain the necessary information, then you will have build or buy a product that allows you to monitor who is viewing which sensitive information.

Alert Example

Sensitive information such as credit card numbers should only be called by a known set of function calls of the web application. If an inappropriate function calls the database for sensitive data or someone is querying the database directly, something fishy is going on. An alert should be sent. The security team should investigate the root cause and take appropriate action depending on the results of the investigation.

Block Escape Routes

Blocking escape routes only when confidential data is on the verge of escaping is difficult to do because a thief can obfuscate the data that is escaping. For instance, a 16 digit number on an email can be detected as a credit card number and blocked from escaping the company; however, a smart thief can disguise the 16 digit number by adding letters in between the digits or simply transforming the 16 digit number into letters or words. Building intelligence into software so it can detect when sensitive data is leaving is challenging.

Design Example

Employees' personal computers can be configured such that some escape routes are blocked. For instance, the personal computer's USB can be disabled for data transfer to a USB memory key and other storage devices. Furthermore, it can be configured to disallow installation of applications such as FTP or other file transferring applications.

An agent can be installed on the personal computer to scan email for sensitive information. This agent can also monitor for sensitive information being pasted into web mail applications. When violations are detected, the action can be blocked and an alert can be sent to the IT security team.

It is important to note that these measures undermine the conveniences that employees are accustomed to having. A simple example is the transfer of a large file between employees. Transfer via email is not possible because the email system rejects big files. All other routes are blocked.

Going Beyond the Examples

There may be clever approaches to block escape routes for only people who have access to sensitive information. Not every person may need to be monitored.

Some development shops in India use the following procedure to ensure that their client's software is protected from theft. Each employee entering the office is searched to ensure that he is not bringing in anything but himself. In the office, he works on a computer that is not connected to the Internet. At the end of the day, he is searched to ensure that he is not leaving with anything from the office.

Encrypt Confidential Information

Confidential information should be encrypted when transmitted on the network, especially public networks where anyone can be eavesdropping.

Conclusion

We covered additional measures that can be taken as lines of defense in addition to the initial safeguards of providing accounts and appropriate privileges to the right people to protect data confidentiality.

Part 3: Compliance

Now that we covered the Cybersecurity Framework and examples of security measures, we are better equipped to understand compliance requirements.

Reading compliance standards for HIPAA or SOX without background knowledge of IT security can be difficult because you are trying to understand abstract guidance.

Part 1 and 2 of this book teaches you an approach to cybersecurity. Part 3 reviews a few selected compliance standards and explains them in a way that leverages cybersecurity concepts already presented.

Lesson 21: PCI DSS - Payment Card Industry Data Security Standard

Introduction

Payment Card Industry Data Security Standard [PCI DSS] was created to ultimately reduce the theft and fraudulent use of cardholder information by providing guidance to merchants on safeguarding the confidentiality of payment card information. The PCI Security Standards Council, the body that created the standard, was established by major credit card companies.

PCI DSS provides many specific technical measures as well as some abstract guidance. With an understanding of parts 1 and 2 of this book, we can fit the measures into the larger context of cybersecurity and “fill in the details” of some of the abstract guidance given in the standard.

Where To Get PCI DSS

The official PCI DSS website is here:

https://www.pcisecuritystandards.org/

As of November 2016, a copy of the latest standard is available here:
https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

A prioritized list of requirements is available here:
https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

PCI DSS's Sensitive Information

The scope of PCI DSS includes all systems and equipment that are potential paths to the compromise of the confidentiality of cardholder information. This includes systems that are not necessarily owned by your organization such as third party systems that your organization relies on.

PCI requires the following sensitive data to be protected:

1. Primary Account Number
2. Cardholder Name
3. Service Code
4. Expiration Date

No other card related data should be stored.

The standard requires measures that are one-time design measures, ongoing maintain/monitor measures, and reaction plan measures that involve technology, people, and processes. In addition, the standard describes methods to test that security measures are actually operating as envisioned. The requirements address security issues of external and internal users.

PCI DSS Requirements Primer

This section helps you understand the thrust of each PCI requirement. The title of each requirement has been rewritten to help you more easily understand the standard.

Requirement 1 – Design your network to be secure

Design your network to be secure. This includes designing the network topology and configuring your perimeter network equipment so that sensitive assets are not easily reached by external users.

Requirement 2 – Configure your hardware to have no default accounts, passwords, and other settings

Using default accounts and passwords on hardware/software systems from firewalls to server operating systems to web servers allow attackers to easily acquire accounts. Never leave default accounts and passwords. Change other default settings that attackers can use to penetrate your systems.

Requirement 3 – Encrypt cardholder data

Store only the data you are allowed to store. Encrypt the data that you do store. Protect your decryption keys.

Requirement 4 – Encrypt cardholder data transmissions

Encrypt cardholder data when transmitting them on public networks.

Requirement 5 – Maintain defense against evil software

Protect against evil software.

Requirement 6 – Maintain defense by patching vulnerabilities

Patch vulnerabilities in operating systems, servers, and applications including your own application – especially if they are exposed to external users.

Use development best practices to develop custom applications so vulnerabilities are minimized and no rogue developer is embedding evil programs.

Don’t mix real cardholder data in the product environment and mock data for development and testing of your application. If you do, you’ll be revealing real cardholder data to your developers.

Requirement 7 – Give accounts to the minimal number of people

Don’t give data access to people who don’t need the data.

Requirement 8 – Manage and protect accounts

Don’t share accounts. Make account passwords hard to guess.

Requirement 9 – Protect your assets in the physical space

Protect your assets in the physical space.

Requirement 10 – Monitor for bad things happening

Use audit data to detect bad things happening. Keep an audit trail of activities and protect the audit trail data.

Requirement 11 – Maintain defenses

Test your defenses periodically. Maintain tools, such as IDS, that you are using to detect bad things.

Requirement 12 – Make defense an ongoing activity throughout your organization

Train your people. Make processes that make protecting the confidentiality of cardholder data a regular part of your organization’s work.

Prioritization

Tackling all 12 requirements at once is challenging. Prioritizing these requirements can help your organization follow a logical trajectory to eventually satisfying the requirements.

From a technical standpoint, it makes sense to design the groundwork of the system to be defensible before adding new monitoring systems on top. Comprehensive documentation should come later; documents, however, should not be completely ignored if writing them helps you get design work done. The design of the system drives how the system will be maintained and monitored. Once the underlying design is stable, investing in monitoring/auditing systems and other systems that run on top of your fundamental design makes more sense.

PCI DSS 3.2 suggests a series of milestones that the organization should achieve. Achieving the milestones involves satisfying a variety of specific "sub-requirements" spread across the 12 requirements.

PCI DSS suggests milestones in the following order:

1. Minimize the amount of sensitive data that you have. Get rid of card data that you are not allowed to store in the first place. Destroy media holding sensitive data when the storing data on media serves no useful purpose.
2. Design your network and systems to be secure and have response plans in place.
3. Design your applications to be secure.
4. Maintain access control by giving accounts only to the right people and monitor the accounts.
5. Design your applications so that sensitive data is encrypted.
6. Design monitoring systems to watch over the system and make maintaining defense of card data an ongoing part of your organization.

Conclusion

It’s important to look at the actual standard itself to understand its details and its prioritization. This lesson serves as a primer to help you avoid getting bogged down in details of the standard.

Lesson 22: HIPAA - Health Insurance Portability and Accountability Act

Introduction

HIPAA was enacted in 1996. The “Security Rule” of Title II of the act describes security safeguards. The safeguards are categorized as:

1. Administrative safeguards
2. Physical safeguards
3. Technical safeguards

Within the cybersecurity space, organizations are required to protect the availability, integrity and confidentiality of electronic forms of protected health information [PHI]. PHI on paper is also protected by HIPAA but in our cybersecurity space, we should concern ourselves with PHI in electronic form.

With an understanding of the Cybersecurity Framework and security measures, we are better fit to understand what to do about HIPAA for cybersecurity.

It is important to note that compliance to HIPAA requires other information technology measures. For instance, the “Transaction and Code Sets Rule” describes how data should be exchanged between different organizations. Furthermore, the Privacy Rule of HIPAA describes how PHI should be handled and these requirements may impact your information technology operations. These topics, however, will not be discussed in this lesson.

The Security Rule will be the focus of this lesson.

Where To Get Security Rule of Title II of HIPAA

The US Department of Health and Human Services website is here: http://www.hhs.gov/hipaa/index.html

HIPAA regulatory standards is available here: http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

Please refer to “Part 164 – Security and Privacy - Subpart C – Security Standards for the Protection of Electronic Protected Health Information” of the document.

HIPAA's Sensitive Information

The Security Rule applies to "covered entities" including health care plans, clearinghouses, and some providers.

HIPAA requires the following 18 types of sensitive patient data (From: Title 45 Code of Federal Regulations 164.514(b)(2)(i)):

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code; and …

HIPAA's Security Rule's Standards Primer

This section helps you understand the thrust of the standards of the Security Rule. Examples of "standard" include "Security Management Process" and "Access Control". Standards fall into three categories of safeguards: administrative, physical, and technical. Under each standard are implementation specifications – a high level "what to do" guide for each standard.

There are two types of implementation specifications: required and addressable. "Required" implementation specifications are required. "Addressable" implementation specifications allow organizations to use alternate implementations to achieve the security standard. Some implementation specifications might not be applicable to some organizations. In this case, the organization does not have to implement the measures, but it must document its decision to not implement them. Please review the finalized rule for details.

This section explains each standard using concepts in parts 1 and 2 of this book, so that they are more easily understood.

1. Administrative Safeguards

Security Management Process

This overarching standard requires that your organization must identify how availability, integrity, and confidentiality of **protected health information** (PHI) can be compromised and take security measures to reduce the likelihood of compromise. Discipline people if you have to.

Assigned Security Responsibility

The organization must clearly designate the person who is responsible for its security program. Assigning clear responsibility assures that the job gets done.

Workforce Security

Make sure the right internal people have access to PHI. Remove access when people should no longer have access to PHI. Access management should be ongoing.

Information Access Management

Make sure that you continue to provide the right access to internal/external applications and external users. Access management should be ongoing.

Security Awareness and Training

Encourage security awareness among your internal users with reminders and training. Training should include measures to protecting against evil software, detecting irregularities in last login data, and using strong passwords. Security can be enhanced through the participation of internal users.

Security Incident Procedures

Have a process and organization in place so that the organization can respond to security incidents. Keep records of the history.

Contingency Plan

Have ongoing processes to backup data. Have a reaction plan including recovery plans and interim operation plan in place for occasions when availability is compromised. Make sure the plan actually works. You want to avoid discovering that there's a glitch in the recovery program when you actually have to recover data.

Evaluation

Adjust security measures to protect PHI as circumstances change. The security program should be ongoing.

Business Associate Contracts and Other Arrangement

Get documented assurances from business associates that they will safeguard shared PHI. Organizations should not ignore how shared PHI is being handled by business associates.

2. Physical Safeguards

Facility Access Controls

Only allow the right people with the right physical access during normal operations and during special operations. During special operations such as disaster recovery, people who

are not allowed physical access during normal operation may need to enter the facility. Keep track of who goes in and out.

Workstation Use

Understand and define what role each workstation or type of workstation should be allowed to take with respect to PHI. If a workstation has a specific role, then you can monitor the workstation to verify that the workstation is not doing stuff it shouldn't be doing.

Workstation Security

Protect workstations in the physical space so only the right people access PHI.

Device and Media Controls

Ensure that PHI on devices and media do not escape. Protect against the physical theft of data.

3. Technical Safeguards

Access Control

Only allow the right people to have accounts that access PHI. Do not share accounts. Accounts that are left with a user logged on should be automatically closed and the user logged off.

Audit Controls

Make sure that your system is operating in the manner expected.

Integrity

Protect against unauthorized changes to data. Make sure that the PHI data being access is the right data.

Person or Entity Authentication

Make sure the right people and organizations are accessing PHI.

Transmission Security

Ensure integrity of PHI is preserved when transmitted. Encrypt transmissions of PHI when eavesdropping is enough of a risk.

Prioritization

The Security Rule does not prioritize the safeguards.

A possible approach to prioritizing the implementation of these safeguards is to identify where the highest risk of compromise is and implement security measures that effectively reduce the risk and are easy to implement.

If you have no physical protection of your sensitive assets, implement barriers to your equipment room. If it's been a very long time since you've checked whether the right internal people have the right access rights to PHI, update your access control assignments. Worry about making this an ongoing process later. If there are no measures to ensure that only the right external users and applications are accessing PHI, then erect network-based and host-based barriers to block unauthorized outsiders.

Conclusion

It's important to look at the actual standard itself to understand its details and history. This lesson serves as a primer. Reviewing parts 1 and 2 of this book will help you understand the context of the Security Rule's implementation specifications and get more concrete ideas of the security measures you should implement.

Lesson 23: Other Compliance Standards: SOX and NERC

Introduction

The Cybersecurity Framework can be leveraged to better understand how to start the cybersecurity component of compliance. This lesson will focus on two more compliance standards, SOX and NERC, and relate them to parts 1 and 2 of this book. The point of this lesson is that the underlying security issues for different kinds of data and IT resources are largely the same although the data and assets of concern are different.

Sarbanes Oxley Section 404 - SOX

You can get a copy of the law here:

http://www.sec.gov/about/laws/soa2002.pdf

You can get more guidance from the SEC about SOX Section 404 for small businesses here: https://www.sec.gov/info/smallbus/404guide.pdf

SOX Section 404 requires adequacy of internal controls over financial reporting.

Auditors may check whether the data entered into the accounting system is true by performing an audit. If the company is depreciating assets, the auditor should check that the assets actually exist. If records show that 5,000 widgets were sold and delivered to Widgets R Us, then the auditor can check that 5,000 widgets were actually delivered to Widgets R Us. Auditors can check that the numbers being entered are real.

While auditors can ensure the entry of truthful data, the cybersecurity team can ensure the integrity of financial data by ensuring that the right people are entering the data and no data is being altered without the knowledge of the organization's rightful authorities. So the cybersecurity measures boil down to safeguarding the integrity of financial data. You must also be able to present evidence that the security measures are working.

North American Electric Reliability Corporation - Critical Infrastructure Protection

You can get a copy of the Critical Infrastructure Protection [CIP] standard here: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx .

This standard concerns itself with safeguarding the availability of **Bulk Electric System** (BES) Cyber Systems and their associated BES Cyber Assets. There is no list of what is included in Cyber Systems and Cyber Assets. Each "Responsible Entity" must determine its own Cyber Systems and Cyber Assets that is in-scope in order to fulfill the standard's requirements.

CIP includes the following sections:

1. *BES Cyber System Categorization*
2. *Security Management Controls*
3. *Personnel and Training*
4. *Electronic Security Perimeter(s)*
5. *Physical Security of BES Cyber Systems*
6. *Systems Security Management*
7. *Incident Reporting and Response Planning*
8. *Recovery Plans for BES Cyber Systems*
9. *Configuration Change Management and Vulnerability Assessments*
10. *Information Protection*
11. *Physical Security*

The approach presented in part 2 of this book to safeguard the availability of assets can help you get a more concrete vision of the security measures you will implement.

Conclusion

You are probably now discovering that the underlying security issues for compliance standards, even ones not mentioned in this book, are similar. They boil down to safeguarding the availability, integrity, or confidentiality of your data or IT assets. Security measures that address the underlying issues can be similar although the specific data and IT assets of concern are different.

You must take measures to address security issues surrounding external and internal users. You must address security issues in the physical and logical spaces. You should have methods of continuously monitoring for potential security breaches and have some kind of reaction plan in store. Giving right people the right level of access control to critical/sensitive data and assets is always an issue.

Parts 1 and 2 of this book cover these common security issues and provide examples of security measures that address these issues. When the specifics of a compliance requirement are unclear, understanding the requirements in the context of the Cybersecurity Framework will help you better judge what security measures are appropriate, build an effective security program, and avoid taking each compliance requirement as boxes to check off a laundry list.

Final Words on Cybersecurity

I believe that the general principles of cybersecurity covered in this book will remain the same in the foreseeable future. The three security goals of safeguarding availability, integrity, and confidentiality probably won't change. You will always have to worry about external users and internal users.

This book describes a way to identify security issues that apply to your organization and provides examples of potential security measures. I hope that this book helps IT professionals relate security measures to security issues. This book should help you avoid getting stuck on the details of security technologies, see the big picture, and assess how vendor technologies fit your needs.

It's important to note that cybersecurity involves not just having technologies, but using technologies the right way. You can buy the most expensive firewall in the market, but if it is not configured correctly, then it is not enhancing security. You can buy the most expensive cybersecurity monitoring system, but it may be looking for the wrong things.

Doing cybersecurity "right" is challenging. cybersecurity is not just a concern of IT professionals of your organization, but requires the participation of all members of your organization and partners who share your IT resources. It's not just about technologies; it's also about expertise.

No matter what compliance standard concerns your organization, I hope that this book gives you a starting point to begin a cybersecurity or compliance programs.

ABOUT THE AUTHOR

Peter Y. Kim earned a BS Electrical Engineering degree and an MS Engineering Economic Systems from Stanford University. He has experience in the IT security industry. He consults for companies that require guidance in starting cybersecurity or compliance programs. He can be reached at pyk@alumni.stanford.edu.