PROMOTING CYBER SECURITY INDUSTRY ON A NATIONAL LEVEL

MAY 9, 2022

EG|CERT

Abstract

In cybersecurity, risk is the potential for loss, damage or destruction of assets or data. Threat is a negative event, such as the exploit of a vulnerability. And a vulnerability is a weakness that exposes you to threats, and therefore increases the likelihood of a negative event.

The most commonly confused terms are risk, threat, and vulnerability. Mixing up these terms clouds your ability to understand how the latest vulnerability management tools and technologies work, and impedes communication with other security (and non-security) professionals. The distinctions may be fundamental, but they're also important.

Table of Contents

Chapter 1

1.1. History

The origin of cybersecurity began with a research project. It only came into existence because of the development of viruses. In 1969, Leonard Kleinrock, professor of UCLA and student, Charley Kline, sent the first electronic message from the UCLA SDS Sigma 7 Host computer to Bill Duvall, a programmer, at the Stanford Research Institute. This is a well-known story and a moment in the history of a digital world. The sent message from the UCLA was the word "login." The system crashed after they typed the first two letters "lo." Since then, this story has been a belief that the programmers typed the beginning message "lo and behold." While factually believed that "login" was the intended message. Those two letters of messages were changed the way we communicate with one another.

In 1970's, Robert (Bob) Thomas who was a researcher for BBN Technologies in Cambridge, Massachusetts created the first computer worm (virus). He realized that it was possible for a computer program to move across a network, leaving a small trail (series of signs) wherever it went. He named the program Creeper, and designed it to travel between Tenex terminals on the early ARPANET, printing the message "I'M THE CREEPER: CATCH ME IF YOU CAN."

An American computer programmer named Ray Tomlinson, the inventor of email, was also working for BBN Technologies at the time. He saw this idea and liked it. He tinkered (an act of attempting to repair something) with the program and made it self-replicating "the first computer worm." He named the program Reaper, the first antivirus software which would found copies of The Creeper and delete it.

After Creeper and Reaper, cyber-crimes became more powerful. As computer software and hardware developed, security breaches also increase. With every new development came an aspect of vulnerability, or a way for hackers to work around methods of protection. In 1986, the Russians were the first who implement the cyber power as a weapon. Marcus Hess, a German citizen, hacked into 400 military computers, including processors at the Pentagon. He intended to sell secrets to the KGB, but an American astronomer, Clifford Stoll, caught him before that could happen.

In 1988, an American computer scientist, Robert Morris, wanted to check the size of the internet. He wrote a program for testing the size of the internet. This program went through networks, invaded Unix terminals, and copied itself. The program became the first famous network virus and named as Moris worm or internet worm. The Morris worm could be infected a computer multiple times, and each additional process would slow the machine down, eventually to the point of being damaged. Robert Morris was charged under the Computer Fraud and Abuse Act. The act itself led to the founding of the Computer Emergency Response Team. This is a non-profit research centre for issues that could endanger the internet as a whole.

Nowadays, viruses were deadlier, more invasive, and harder to control. We have already experienced cyber incidents on a massive scale, and 2018 isn't close to over. The above is to name a few, but these attacks are enough to prove that cybersecurity is a necessity for corporations and small businesses alike.

1.2. Definition

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.

1.3. Why is Cybersecurity Important?

Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.

Both inherent risk and residual risk are increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber-attack or data breach is on the rise.

Business leaders can no longer solely rely on out-of-the-box cybersecurity solutions like antivirus software and firewalls, cybercriminals are getting smarter, and their tactics are becoming more resilient to conventional cyber defenses. It's important to cover all the fields of cybersecurity to stay well-protected.

Cyber threats can come from any level of your organization. Workplaces must include cybersecurity awareness training to educate staff about common cyber threats like social engineering scams, phishing, ransomware attacks (think WannaCry), and other malware designed to steal intellectual property or personal data. The proliferation of data breaches means that cybersecurity is not just relevant to heavily regulated industries, like healthcare. Even small businesses are at risk of suffering irrecoverable reputational damage following a data breach. To help you understand the importance of cyber security, we've compiled a post explaining the different elements of cybercrime you may not be aware of. If you're not yet worried about cybersecurity risks, you should be

Chapter 2

2.1. Cybersecurity Goals

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals:

- **Protect the confidentiality of data.**
- **Preserve the integrity of data.**
- **Promote the availability of data for authorized users.**

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the AIC (Availability, Integrity, and Confidentiality) triad to avoid the confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

2.1.1. Confidentiality

Confidentiality is the process that rules out access to information to certain people. It is a measure to restrict sensitive information from getting into the wrong hands. In an organization, people are allowed or denied access to information according to their occupation. This kind of people get proper training and rules about the sharing confidential secrets, secure their accounts with properly strong passwords. Some of the key points of what is cybers security made of are 2FA (two-factor authentication, data classification, data encryption, biometric verification, etc.

Tools for Confidentiality:

i. Encryption

Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key). It protects sensitive data such as credit card numbers by encoding and transforming data into unreadable cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the two primary types of encryption.

ii. Access control

Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users need to present credentials before they can be granted access such as a person's name or a computer's serial number. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

iii. Authentication

An authentication is a process that ensures and confirms a user's identity or role that someone has. It can be done in a number of different ways, but it is usually based on a combination of:

- **something the person has (like a smart card or a radio key for storing secret keys),**
- **something the person knows (like a password),**
- **something the person is (like a human with a fingerprint).**

Authentication is the necessity of every organizations because it enables organizations to keep their networks secure by permitting only authenticated users to access its protected resources. These resources may include computer systems, networks, databases, websites and other network-based applications or services.

iv. Authorization

Authorization is a security mechanism which gives permission to do or have something. It is used to determine a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. System administrators are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

v. Physical Security

Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

2.1.2. Integrity

The process of integrity assures that the data in the system is consistent, verified, accurate and trustworthy. It means that the data cannot be changed, altered, deleted, or accessed without certain permission. This is why it is important to keep track of file permissions and user access. Another important thing to maintain data integrity is to have a secured backup. Cloud backups are one of the most trustworthy at this time.

Tools for Integrity

I. Backups

Backup is the periodic archiving of data. It is a process of making copies of data or data files to use in the event when the original data or data files are lost or destroyed. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy. Many applications especially in a Windows environment, produce backup files using the .BAK file extension.

II. Checksums

A checksum is a numerical value used to verify the integrity of a file or a data transfer. In other words, it is the computation of a function that maps the contents of a file to a numerical value. They are typically used to compare two sets of data to make sure that they are the same. A checksum function depends on the entire contents of a file. It is designed in a way that even a small change to the input file (such as flipping a single bit) likely to results in different output value.

III. Data Correcting Codes

It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

2.1.3. Availability

In terms of necessary components like hardware, networks, software, devices, and equipment, availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. Utilities like firewalls, proxy servers, backup solutions, and recovery plans are key points against cyber threats. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools for Availability:

I. Physical Protections

Physical safeguard means to keep information available even in the event of physical challenges. It ensures sensitive information and critical information technology are housed in secure areas.

II. Computational Redundancies

It is applied as fault tolerant against accidental faults. It protects computers and storage devices that serve as fallbacks in the case of failures

Chapter 3

3.1. Defining the Components of Cybersecurity Risk

3.1.1. An asset

- Anything of value to critical cybersecurity infrastructure. This includes not just systems, software, and data, but also people, infrastructure, facilities, equipment, intellectual property, technologies, and more.
- Creating inventory and assessing the value of each asset is a vital first step in risk management.
- It's essential in order to accurately assess risk (how do you know what's at risk if you don't know what you have?) and then determine what type and level of protection each asset needs.

3.1.2. Vulnerability

- Vulnerability is any weakness (known or unknown) in a system, process, or other entity that could lead to its security being compromised by a threat.
- Vulnerabilities can exist almost anywhere, from hardware devices and infrastructure to operating systems, applications, modules, drivers, software, and web applications.
- Also, there are (*Zero-day* vulnerabilities refers to a newly discovered vulnerability for which a patch does not yet exist.)

3.1.3. Threat

- A threat is any action (event, occurrence, circumstance) that could disrupt, harm, destroy, or affect an information system (and thus, an organization's business and operations).
- A threat is anything that could compromise confidentiality, integrity, or availability of systems or data.

3.1.4. Exploit

- Exploit means to take advantage of vulnerability. An exploit refers to a tool, typically in the form of source or code.
- This code makes it easy for threat actors to take advantage of a specific vulnerability and often gives them unauthorized access to something (a network, system, application, etc.).
- The payload, chosen by the threat actor and delivered via the exploit, carries out the chosen attack, such as downloading malware, escalating privileges, or exfiltration of data.

3.2. Accurately Assessing Risk

Let's define the two essential elements of risk calculations that are often overlooked.

3.2.1. Likelihood

- Likelihood is the chance or probability that a specific threat will exploit a specific vulnerability. Factors that figure into likelihood include things like a threat actor's motivation and capabilities, how easily a vulnerability can be exploited, how attractive a vulnerable target is.

- If exploit code exists for a specific vulnerability, the attacker is skilled and highly motivated, and the vulnerable target system has few security controls in place, the likelihood of an attack is potentially high. When the opposite of any of these is true, likelihood decreases.

3.2.2. Impact

- Impact describes the damage that could be done to the organization and its assets if a specific threat were to exploit a specific vulnerability.
- Obviously, some assets are more valuable to an organization than others.
- Assuming a matched vulnerability and threat exists, it's essential to consider *both* likelihood and impact to determine the level of risk.
- A simple, qualitative (versus quantitative) risk matrix like the one shown in Figure illustrates the relationship between the two.

Likelihood \ Impact	LOW	MEDIUM	HIGH
HIGH	Medium risk (3)	High risk (4)	Highest risk (5)
MEDIUM	Low risk (2)	Medium risk (3)	High risk (4)
LOW	Lowest risk (1)	Low risk (2)	Medium risk (3)

Chapter 4

4.1. Developing an Effective Security Strategy

- Security should be built into the culture of your organization to ensure that every employee within the organization understands the importance of cyber security and the far-reaching impact that a data breach can have.
- However, Human error remains the number one cause of a cyber-attack and cybercriminals are quick to take advantage of this lack of cyber security awareness to launch a targeted attack. The development of a comprehensive security strategy will protect sensitive data, reduce threats and ensure the reputation of an organization remains intact.

4.2. Developing a Cyber Security Strategy

- Every strategy should be custom-designed. A cybersecurity strategy that works for one organization will not necessarily be effective for another. It's different for every entity based on their specific needs and vulnerabilities.
- However, there are some factors that you can consider regardless of your organization's size, scope, or industry.

4.2.1. Understanding risks to critical operations

- Cybersecurity is continually becoming more complex. Organizations must have a 'security vision' about what cybersecurity means to their operations.
- This includes generating an acceptable level of risk and prioritizing areas to target for the majority of security investments.

4.2.2. Define the threats on the inside

- Many of the backdoors and vulnerabilities that cause an organization to be a victim to cyberattacks begin from an internal problem.
- A part of every cybersecurity package should include internal monitoring to prevent insiders from using their access maliciously.

4.2.3. Plan for breaches ahead of time

- Understand that attackers are always one step ahead of the curve in security. No matter how good your defenses may be, they will be breached at some point in time.
- So, preparation for the attack will enhance the disaster recovery and business continuity measures so that when something does happen, you can return to normal functionality as quickly as possible.
- With the basics of cybersecurity covered, should an organization now feel relaxed? Not at all. The defenses that work today will not work tomorrow. Attackers will have figured out something else by then, and they will be at your front door with even more powerful executions.
- So continuous preparation and learning, also the concept of threat hunting and working in a proactive way is important

4.3. Keep Defensive Practices up to date

- Security policies could be rendered useless unless organizations have a thorough and continual way of monitoring cyber security compliance.
- The security landscape is constantly shifting and evolving so it is vital that employees are continually trained to ensure they can respond appropriately to the most up to date security threats.

4.4. Security Awareness Training

- Effective security awareness training is essential in training staff on how to identify and respond appropriately to the growing range of cyber security threats.
- All employees, at every level of the organizations should receive this training to ensure they have the skills required to identify an attack.
- Cyber Security awareness training should be engaging and informative to ensure that staff understands what is required of them and the importance of their role in safeguarding the organization's sensitive data.

4.4.1. Security awareness training will:

- Educate staff on the cyber threats faced.
- Raise awareness of the sensitivity of data on systems.
- Ensure procedures are followed correctly.
- Provide information on how to avoid Phishing emails and other scam tactics.
- Reduce the number of data breaches; Build a culture of enhanced security compliance.

Chapter 5

5.1. Guide organization to Follow Cybersecurity Framework

- The cybersecurity framework helps organizations better understand, manage, and reduce their cybersecurity risk and protect their networks and data.
- The Framework gives the organization an outline of best practices to help decide where to focus time and investments for cybersecurity protection.
- The Cybersecurity Framework addresses five areas: Identify, Protect, Detect, Respond, and Recover.

5.1.1. IDENTIFY

- Make a list of all equipment, software, and data used, including laptops, smartphones, tablets, and point-of-sale devices.
- Create and share an organization cybersecurity policy that covers:
  - Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.
  - Steps to take to protect against an attack and limit the damage if one occurs.

5.1.2. PROTECT

- Control who logs on to the network and uses computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity.
- Help employees understand their personal risk in addition to their important role in the workplace.

5.1.3. DETECT

- Monitor devices for unauthorized personnel access, devices (like USB drives), and software.
- Check network for unauthorized users or connections.
- Investigate any unusual activities on the network.

5.1.4. RESPOND

- Have a plan for:
  - Notifying customers, employees, and others whose data may be at risk.
  - Keeping operations up and running.
  - Reporting the attack to law enforcement and other authorities.
  - Investigating and containing an attack.
  - Updating your cybersecurity policy and plan with lessons learned.
  - Test your plan regularly.

5.1.5. RECOVER

After an attack:

- Repair and restore the equipment and parts of network that were affected.
- Keep employees and customers informed of the response and recovery activities.
- Keep monitoring recovered systems for a period of time to observe any abnormal behavior that could indicate re-infection of these systems.