Cybersecurity Basics

Section II

SELF PACED | ON-DEMAND | INSTRUCTOR-LED | COLLABARATE | SHARE

Vivaan-lms

A new way of learning

p:972-591-8515 | WWW.VIVAANLMS.COM

Table of Contents

CHAPTER 1: CYBER SECURITY

- Introduction to Cyber Security
- Understanding Internet governance
- Identity and authentication on the Internet
- What do we mean by security?
- What are cyber threats?
- What are the vulnerabilities?
- Building trust in cyberspace
- What is an advanced persistent threat?
- Basics of computer defense
- Who is the weakest link?
- Why security awareness for end users is so important – a close look at phishing.
- Security awareness to protect against phishing
- A realistic approach to training employees
- What cybersecurity policies should include
- The Principle of Data Collection

INTRODUCTION TO CYBER SECURITY

"It's not a truck, it's a series of tubes".

This is how a senator from Alaska had famously described the cyberspace at a congressional hearing. At the time, the senator was mocked for calling cyberspace a series of tubes, whereas in fact it is rather difficult to define ideas in terms of cyberspace. "Tubes" is actually a mangling of the idea of "pipes," an analogy that is used by experts in the field to describe data connections.

Part of why cyberspace is difficult to describe and understand today is because of its global and expansive nature. The cyberspace has changed drastically and also almost unrecognizable in comparison to its humble beginnings. The US Department of Defense can be considered the godfather of cyberspace, referring back to its funding of early computing and original networks like ARPANET.

There have been several definitions for cyberspace over the years, but at its essence, cyberspace is a realm of computer networks and the users behind them in which information is stored, shared and communicated online.

Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. But cyberspace isn't only virtual. It consists of computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, mobile technologies, fiber-optic cables, and space-based communications.

Cyberspace is constantly evolving. Since humans and technology use the cyberspace, as there are changes to both these factors, the cyberspace also changes drastically. It may have initially started off as being just a communication realm, but today with the rise of e-commerce and other uses of the Internet, cyberspace has gone on to become 'critical infrastructure'. Cyberspace has almost now become 'the dominant platform for life in the 21st century'. But the Internet we have all grown to become so dependent on for various purposes is increasingly coming under danger.

UNDERSTANDING INTERNET GOVERNANCE

In 1998, Jon Postel, a respected computer researcher and leader sent an email to eight people. He asked them to reconfigure their servers so that they would direct their Internet traffic using his computer at the University of Southern California rather than a computer in Herndon, Virginia. These eight people did as they were told without asking any questions. This switch made by Postel was done so without any permission. Basically, he did this to prove to the then US Government that the Internet cannot be controlled as they please and take away control from the wide set of researchers who had worked on it.

Postel's little experiment for the very first time exposed that the Internet has governance issues. Eric Schmidt later made a statement saying "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." Since digital resources are not scarce as traditional ones, its governance also will be done differently.

IETF (Internet Engineering Task Force)

The operations of the Internet require independent actors to follow basic rules that guarantee interoperability, known as standards. This standards-based approach traces back to the beginning of the Internet. Eventually IETF (Internet Engineering Task Force) was developed that is a set of new Internet standards and protocols and modifies the existing ones for better performance. Everything developed by the IETF falls under specific working groups that concentrate on areas like routing, applications, and infrastructure.

Openness is critical to the culture of IETF. In some working group meetings, the members decide on an issue by humming for or against a proposal. While the IETF has no official board or formal leadership, the Internet Engineering Steering Group (IESG) offers oversight and guidance for both the standards process and the standards themselves.

The Internet Society (ISOC)

The Internet Society (ISOC) is an international group that formed in 1992, which oversees most of the technical standards and processes. The ISOC was set up as an independent, international organization to provide a formal, legal means to safeguard the independent and open standards processes. With all these informal and semi-formal groups floating around, there was still a shadow in Internet governance and safety.

Internet Corporation for Assigned Names and Numbers (ICAAN)

The growing pressure for commercial Internet lead to the fact that the US government cannot govern Internet. Soon ICANN (Internet Corporation for Assigned Names and Numbers) was born. ICANN put in place a more structured way to distribute IP addresses that more reflected on the Internet's global nature. Despite efforts to globalize Internet governance, many still see ICANN as captive to US interests. With no other alternative right now, we can't really criticize ICANN.

With all these various governance issues, it's safe to say that the Internet has always defied traditional governance models.

IDENTITY AND AUTHENTICATION ON THE INTERNET

It is essential to separate identification from authentication. Authentication acts as proof of identification.

Identification

Identification is the ability to identify uniquely a user of a system or an application that is running in the system.

Authentication

Authentication is the ability to prove that a user or application is genuinely who that person or what that application claims to be.

- **Examples of Authentication and Identification**
  For instance, bank ATMs have cards for identification, whereas in recent times, the mobile phone acts as an authenticator. One-time codes received on the registered mobile phone acts as authenticator for the particular financial transaction.

Authorization

After authentication comes authorization. What can be done after the system you are using has identified you. Obtaining authorization can open doors to more opportunities. Authorization is the part that links these technical issues to policy, business, and political and moral questions.

Digital Identity

Digital identity is a balance between protecting and sharing information for the purpose of cybersecurity. Limiting access of acquired information gives rise to privacy of that particular information, plus it prevents more sophisticated fraud.

WHAT DO WE MEAN BY SECURITY?

In the earlier days of the computer, there was a joke going around on the security perspective as to how one can keep the data on the computer safe. 'Just unplug it'! By keeping the system unplugged it was believed it can be kept safe. But jokes aside, we do know that today with wireless and rechargeable devices, once a machine is plugged in, it can always deviate from its intended purpose.

Security is not just a thought of being free from threat, but it is also the presence of an adversary. A cyber problem becomes a cybersecurity issue if the adversary seeks some information from the activity, thereby making it a data breach.

In the digital world, protecting information is of huge importance. Privacy is an important factor and sensitive data and classified data must be kept confidential. In case of a data breach, the adversary gaining the information can get a lot of information that can put the user at risk. Keeping data confidential can be done through tools such as encryption and access control.

Integrity

Integrity is a critical factor in data security. Integrity, in terms of cybersecurity means that the system and the data it contains have not been improperly changed without authorization. A user needs to have confidence in the system that it will behave as expected and be available when required.

Integrity is a very subtle factor in security because it is challenging to realize if the system is behaving in the manner expected. An attacker can disable a system and make it inaccessible for a user.

Security costs money, but it also costs time, convenience, capabilities, liberties, and so on. All of these aspects of security are not just technical issues: they are organizational, legal, economic, and social as well. But most importantly, when we think of security we need to recognize its limits.

WHAT ARE CYBER THREATS?

Cyber attacks in 2017 alone have caused a damage worth about $5 billion. This is only set to increase in the coming years with cybercrime damage expected to hit $6 trillion annually by 2021.

Cyber Threat

A cyber threat is a malignant and destructive act that tries to gain access to one's system or data without authorization. A cyber threat takes place through the computer network. Cyber attacks are carried out by people termed as 'hackers' who gain unauthorized access to your system thereby stealing sensitive important data and cause harm to your system.

Listed below are some of the common cyber threats taking place today -

1. **Advanced Persistent Threats (APT) –** An APT attack is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time for the purpose of stealing data.

2. **Email Malware –** Email Malware is also known as email spam and spreads unwanted and unsolicited email and is often started and solicited through links in the messages that leads to phishing websites and other sites that host malware. Email Malware can act as an agent that allows attackers to attack other computers through your computer. Email malware comes in many forms but essentially can steal data from your computer such as bank logins, passwords, or files and can detrimentally take full remote control of your computer.

   Here are some of the flavors of email malware:

   a. ***Ransomware*** – Encrypts the victims data and demands a fee to restore it.

   b. ***Phishing*** – Uses authentic looking senders with a socially engineered message to coax the victims to release sensitive data.

   c. ***Spear Phishing*** – Targeted phishing attempts for a specific organization where cybercriminals prepare extensive prior research to appear authentic and legitimate.

   d. ***Spoofing*** – Hackers use addresses and domains that are similar to legitimate ones to deceive victims into believing fraudulent emails are from a trusted individual.

   e. ***Man-in-the-Middle Attacks*** – Cybercriminals insert themselves between the user and the application, website or service that the victim is using and enables the attacker to impersonate the victim, steal valuable personal information and read, manipulate and send emails without the victim's knowledge. Cybercriminals can even modify or conduct transactions with this type of tactic.

f. ***Whaling/Business Email Compromise (BEC)*** – The term whaling is used to indicate the that cybercriminals target the largest fish in the organization who has the decision-making power to carry out financial transactions. These emails look like they come from the CEO or other higher management and requests immediate financial transactions such as direct deposits, wire transfers, or vendor payments or purchases.

g. ***Spam*** **–** Spam email often contains malware and dangerous malicious content.

h. ***Key Loggers*** **–** Keyloggers are often obtained when cybercriminals send victims a malicious email and they inadvertently click on the malicious attachment or link causing a stolen user credential or identity.

i. ***Zero-Day Exploits*** **–** A cyber attack that occurs the same day a security weakness is discovered in software and is exploited before a patch or fix is available. This type of exploit is often delivered via malicious email to help them gain authorization and ultimately to steal sensitive information.

j. ***Social Engineering*** **–** Cybercriminals impersonate trusted individuals to build up trust and engage in conversation to gain access to a company's network.

3. **Trojans –** A type of malware that is often disguised as legitimate software to help cybercriminals gain access to users' systems. This is often used in conjunction with social engineering to trick users into loading Trojans into their systems.

4. **Botnets** – A network of interconnected private computers or devices that are infected with malicious software and controlled and coordinated as a group without the owner's knowledge so that the cybercriminals can access the network to perform malicious activities such as stealing data, sending spam, and performing DDoS (distributed denial-of-service attack), just to name a few.

5. **Ransomware** – Ransomware is a common and dangerous cybersecurity threat wherein a user is denied access to their system or a website, and access can only be regained after paying a certain amount of money as ransom to unlock the system. In general, ransomware is a form of malicious software or malware that prevents you access to your data unless you forgo some sort of ransom fee via an untraceable bitcoin payment for the cybercriminal to restore your access to the data. One of the common delivery systems of ransomware is phishing email spam attachments that are disguised as trusted files. A common type of ransomware is often to encrypt some or all of the user's files and can only be decrypted by a mathematical key known only by the attacker.

    a. **Leakware or doxware:** A less common variant of ransomware where the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. However, this tactic is usually only used a threat as finding and extracting information is tricky for attackers so encryption ransomware is the most common form.

6. **Distributed Denial of Service (DDoS):** A DDoS is when multiple compromised computer systems attack a target, such as a server, website or other network resource causing a denial of service for users of the target resource.

7. **Wiper Malware Attacks:** A wiper malware is intended to wipe the hard drive of the computer it infects.

8. **Intellectual Property Theft (IP theft):** Intellectual property theft is stealing of trade secrets, trademarked materials, designs or ideas as well as copyrighted materials such as music, drawings, or information.

9. **Theft of Money:** Stealing of Money

10. **Data Manipulation:** Some refer to this as the latest technique in the "art of war in cyberspace" where the cybercriminal alters digital documents and other information that could lead to disaster

for corporations, health care organizations, the governmental agencies, and other individuals.

11. **Data Destruction:** Cybercriminals permanently destroy, erase, and wipe out the entire database of an entire corporation. They may do this by destroying data on hard drives, memory cards, smartphones, and other mobile devices. The worst cyber attack in history occurred in 2012 with the oil giant Saudi Aramco involving data destruction where the hard drives of more than 30,000 desktops and servers were attacked by malware and aimed to wipe out the entire IT infrastructure of Aramco.

12. **Spyware/Malware:** Malware are malicious software designed to cause damage to computers or networks. Spyware software monitors your computer and reveals collected information to the cybercriminal.

13. **Man-in-the-Middle (MITM):** A example of man-in-the-middle attacks is actively eavesdropping where the attacker secretly relays and possibly alters communication between parties who believe they are directly communicating with each other.

14. **Drive-By Downloads:** Unintentional downloading of software sometimes caused by just opening up an infected website by visiting it (driving by). Drive-by Downloads can also exploit a browser, app or out-of-date operating systems that has a security vulnerability.

15. **Malvertising:** This involves online advertising to spread and interject malicious malware filled advertisements into legitimate online advertising networks and web pages.

16. **Rogue Software:** This is a malicious software that tricks the user into thinking that their system has malware or viruses on it and thus manipulates the victims into paying money for a fake malware or virus removal tool where it actually introduces malware into the computer.

17. **Unpatched Software:** Software that has vulnerabilities that cybercriminals can exploit.

18. **Social Engineered Malware (SEM)**: An attack that tricks users into downloading and installing malicious software that compromises the security of their system.

Most Common Sources of Cyber Threats:

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

Types of Social Engineering Attacks:

- ***Phishing*:** Attackers use emails, social media, instant messages, and SMS to trick victims into providing sensitive information or in visiting malicious URLs for the purposes of compromising systems.
- ***Watering Hole*:** Injecting malicious code into public Web pages of a site that the targets normally

visit. This type of attack is common for cyber espionage operations or state-sponsored attacks.

- ***Whaling Attack*:** The choice of targeted victims distinguishes this category of targets which happen to be relevant large executives of private business and government agencies, thus the use of the term whaling.

- ***Pretexting*:** The practice of presenting oneself as someone else (impersonation) to obtain private information. Oftentimes, attackers will create a fake identity, build up trust, and use it to manipulate victims to coax them for sensitive information.

- ***Baiting*:** This type of hacking exploits human curiosity and is characterized as the promise of a good deed. However, this is a launch point for which hackers use to deceive victims. An example is when attackers use a malicious file disguised as a software update or generic software.

- ***Quid Pro Quo*:** An iteration of the baiting attack and means "something for something". The difference is instead of baiting the victim with the promise of a good, a quid pro quo attack promises a service or benefit based on the execution of a specific action. For example, the hacker offers a service or benefit in exchange for information or access. The most common one occurs when a hacker impersonates an IT staff of a large corporation and could be calling employees of the target company and offers them some kind of upgrade or software installation.

- ***Tailgating*:** This is also known as piggybacking where an attacker seeks entry into a restricted area that lacks proper authentication. A typical situation happens when an attacker simply walks behind a person who is authorized to access the area or impersonates a delivery driver or caretaker who is packed with parcels and asks the person to hold the door, evidently bypassing the electronic access controls.

What are the Vulnerabilities?

Security Vulnerability
A security vulnerability is a weakness in a product or system that attackers capitalize on and further compromise the system's integrity, confidentiality and availability.

Three Main Goals of Vulnerability
Integrity, availability and confidentiality are the three main goals of security. If any of these is compromised, you have a security vulnerability. A single security vulnerability can consist of any one of these elements or all three of them.

1. **Integrity** - trustworthiness of a resource is termed as integrity. In a situation of a security breach, the attacker is trying to compromise this trust without authorization, thereby compromising on integrity.

2. **Confidentiality** - limiting access to information to only specific set of people is termed as confidentiality. An attacker will try to compromise this element by accessing information that he is not privy to.

3. **Availability** - the possibility to access a particular resource is termed as availability. When an attacker denies permission to access a particular resource, the availability has been compromised.

Common Security Vulnerabilities

- ***Injection*** - includes all kinds of vulnerabilities where an application sends untrusted data to an interpreter
- ***Broken authentication*** - involves flaws that are caused by error in implementations of authentication and/or session management
- ***Sensitive data exposure*** - a flaw wherein an application allows easy access to sensitive data
- ***Broken access control* -** flaws including weak access control to applications which should not be

allowed for all users

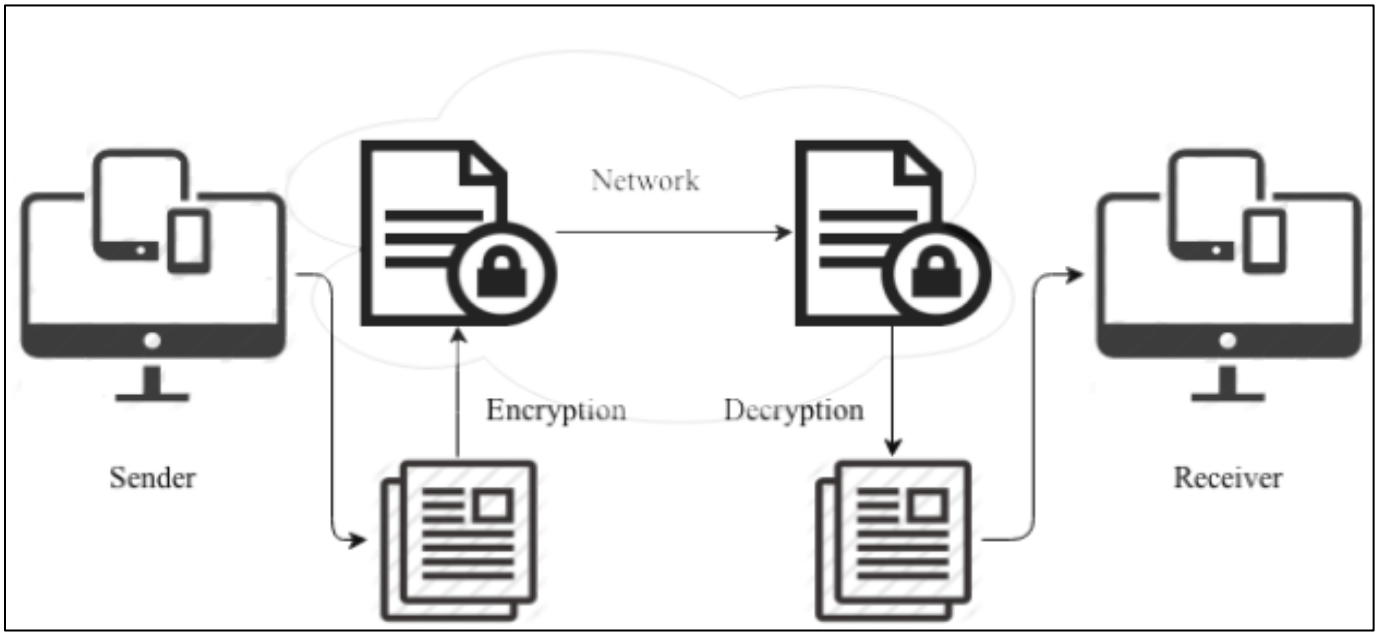
- ***Security misconfiguration* -** occurs due to poor configuration in a system making it more insecure and vulnerable to attack
- ***Insufficient logging and* monitoring -** lack of best practices that should be in place to check for security breaches

Building Trust in Cyberspace

With the continuous rise and rapid adoption of the digital world, online trust becomes a critical factor. For cybersecurity, the users must know how to trust the system and the system must know how to trust the users.

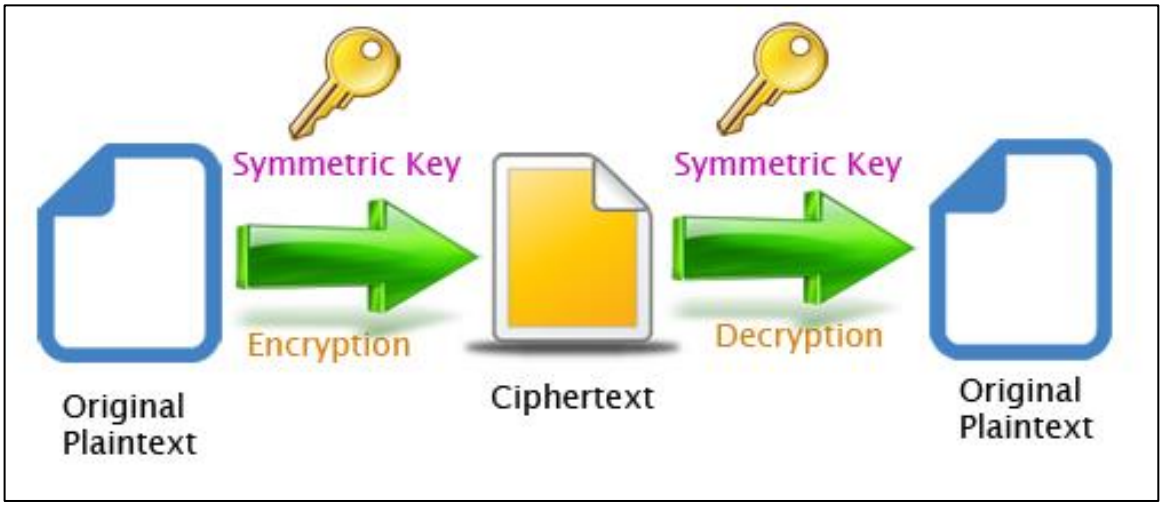
- ***Online trust is built through cryptography* -** The practice of secure communications that dates all the way back to the first codes that Julius Caesar and his generals used to keep their enemies from understanding their secret messages. Cryptography keeps information confidential and also has the ability to detect any tampering of data.

Figure 1.1: Process of Cryptography



Modern cryptography methods rely on 'keys' for the encryption and decryption process. Symmetric encryption relies on one single key that both end users trust for encryption and decryption.

Figure 1.2: Keys in Cryptography



A user can be authorized to use a system after identification and authentication is complete. Most systems use some kind of "access control" to determine who can do what. At its simplest, access control provides the ability to read, write, or execute code in an operating environment. Good access control policies are essential for any organization. Failure of access control systems has been one of the key reasons for some of the biggest cybersecurity scandals recently.

What is an Advanced Persistent Threat?

Advanced Persistent Threat (APT), is carried out by professional hackers whose full-time job is to carry out a specific hack on a company/ target. APTs work for either the government or relevant industries. These hackers carry out specific instructions given by their client for the hack.

***These specific hacks include*:** accessing confidential information, placing destructive code, or placing hidden backdoor programs that allow them to sneak back into the target network or computer whenever they wish to.

A successful APT is one wherein the hacker breaks into the network and computer and takes the information needed and leaves unnoticed. APTs do not cause any drastic changes in the network for users to get suspicious.

Signs to look out for during an APT attack -

- **Increase in system log-on at night** - APT hackers usually are in the opposite side of the world attempting a hack on a network on the other side of the globe. If you notice a spike in the log-ins on a network which is at night time and not in use, then it could be an APT.

- **Widespread backdoor Trojans** - APT hackers usually install a backdoor Trojan which will help them to get back into the system whenever they wish to.

- **Unexpected information flow** - Keep an eye out for unusual amounts of information being transferred from your network to an external system.

- **Unexpected data bundles** - look out for large chunks of data appearing suddenly in places where they aren't supposed to be

BASICS OF COMPUTER DEFENSE

The advantage of defending a computer system is that once you know what might attack you, you can just tell the computer what to watch for and how to avoid it. Traditional antivirus software relies on detecting these "signatures." The programs scan all files on the system as well as incoming traffic against a dictionary of known malware, looking for anything that matches these signatures of malice.

Modern antivirus doesn't just screen, they use "heuristic" detections to identify suspicious computer code behavior based on rules and logical analysis. Static analysis breaks apart the computer code and looks for patterns associated with the behavior of an attacker. Virtual machines and other sophisticated defenses dynamically simulate the code operation to determine whether the file examined will misbehave without putting the actual system at risk.

Firewall

The simplest form of network defense is a "firewall." Firewalls can prevent external computers from connecting to the firewalled machines except under pre-set circumstances or prevent certain applications on the computer from opening network connections.

"Intrusion detection systems" exist at the computer level or on the network. They detect attack signatures and identify anomalous behavior.

Air Gap

In cybersecurity terms, an air gap is a physical separation between the network and critical systems. Such practice is common with critical infrastructure, such as with power companies.

Who is the weakest link?

It's time to stop blaming employees and enlist their help. As the old saying goes, "people are the weakest link in the cybersecurity chain." Clearly, enterprise security professionals agree with this statement, as it turns out that 58% point to a "lack of user knowledge about cybersecurity risk" as being one of the highest factors most responsible for successful malware attacks. Therefore, end users must be part of the cyber security solutions and rigorous continuous training must be in place. When a user makes a mistake and clicks on an email that causes an infection, we often think that was the root cause. However, in actuality, the organization was already under attack when the attacker sent the email before it was opened. This proves that every other security control in the path of that attack had failed.

The real battle in cybersecurity is not just about high technology. It is also driven by the human factor, the fight over our behavior. It is for this reason that many IT experts believe that if a network has any kind of sensitive information in it, all users need to be regularly certified in cybersecurity basics. This means every- one, from junior staff all the way up the leadership. Build constant awareness, reinforcing it with new training. If users fail to learn the lessons of proper caution, then their access privileges should be revoked.

WHY SECURITY AWARENESS FOR END USERS IS SO IMPORTANT – A CLOSE LOOK AT PHISHING

If you could use one word to sum up why security awareness is so important for end users it would be: "phishing" because it is a very common attack for end users.

For those who are unaware of the term, the definition of phishing is any ploy to solicit sensitive information (i.e. passwords, social security numbers, etc.) by pretending to be an authority figure, trusted or familiar person.

Classic Examples of Phishing

A classic example would be when a person receives an email with their "new password" from an individual claiming to be from the IT department. When the recipient responds that they've compiled and changed their password, the cybercriminal can strike and have access to that person's email address and can use it for all kinds of malicious or nefarious purposes.

Sadly, this is only one of the countless versions of phishing. Sometimes emails will come from banks or seller platform accounts like eBay or Amazon, claiming that you have violated a rule and that your account will be shut down, or that you have just bought this item, it looks authentic and because of the fear factor that comes out of thinking that your account will be shut down, users sometimes click on the email. Some have come in the form of examples like iTunes, or the most obvious to spot is the ones that claim you have won a lottery from a foreign land. For those that are well informed, they can easily spot these things, however, the cybercriminal is looking for weak victims and they will send out masses of these emails hoping that they can catch someone naïve and vulnerable, including the elderly and uninformed. Tactics used in conjunction with sending out phishing emails include scare tactics to get the person to check their account and click on links within the email. When in doubt never click on these emails at all. You can open up a new browser and login yourself to check your account or balance. The emails should always address the person by name and business and will never ask for personally identifying information like birthdates or social security numbers on them.

To actually be a hacker takes an impressive degree of technical acumen and skill. With this technical knowledge and skill, many cybercriminals could find legitimate employment in just about anywhere in the IT field, but unfortunately, they take their skills and use them in crime.

The scariest element of a phishing attack is that anyone can do them and they can be absolutely brutal in terms of fallout consequences. On the other hand, all it takes is an email address, or just a phone number and a weak moral character to be successful with phishing. Phishing is a numbers game that usually favors the criminal, so even if the cybercriminal is unsuccessful at first, they have a number of employees to attempt their scheme.

Long-Term Effects of Phishing

Phishing can bring on long-term effects and damage down the organization and the damage may go unnoticed for a long time. Accessing a low-level employee's email inbox may not seem like it would have such dire implications, but at least for some time, the criminal will be able to impersonate their victim, which could lead to gaining plenty of sensitive information.

Spearfishing – this type of spear phishing attack is a far more precise and sophisticated ploy and takes far more research on behalf of the criminal to impersonate someone specifically. Thus, cybercriminals

need to figure out certain details about the victim to make this possible. They will do intensive frontend research on the victim. Therefore, they may go through the target victim's Facebook, LinkedIn, and other online social media profiles to ensure that they come across as believable as possible.

Security Awareness to Protect Against Phishing

The truly frustrating thing about phishing attacks is that they should be so easy to protect against, but because of carelessness, letting down one's guard, and ignorance, thousands of people fall victim every day. Always make sure you know who is sending you an email and if they ask for anything even remotely suspicious, call them to make sure they are indeed the ones who sent the message. This may seem trivial, or might seem unnecessary, but you'd rather be safe than sorry. It only takes a minute to call to verify rather than spending countless hours, headaches, and potential damages to your entire corporation just because this could have been avoided by stepping back to think about the situation. So, the rule is: Think before you click! And practice this every day, at work and at home!

The first step is awareness. Your entire organization needs to understand what phishing scams involve and what to look for so they are not fooled.

Make sure that personnel understand the consequences of falling for such a scheme. Again, phishing can lead to all kinds of bigger problems. The idea is to get your people to take these sorts of attacks seriously. If they don't, your corporation will become a victim.

Encourage people to come forward when they think they have been targeted. No one should ever feel embarrassed for coming forth with a report of breaches or suspicion. Time is of the essence, the more time that passes after a suspicious attack has been suspected, the more time the cybercriminal has time to do detrimental things that could lead to long-lasting consequences.

Schedule regular calendar events, activities, programs and reminders that phishing is a threat so your staff is intimately aware of it.

Factors Contributing to Successful Phishing Attacks:

These attacks only work when people

1. Let down their guard
2. Assume something is safe without verifying the source
3. Are careless
4. Ignorant and uninformed people, and
5. People are not being vigilant.

Figure 1.3: Think Before You Click

A REALISTIC APPROACH TO TRAINING EMPLOYEES

So, we know that humans are the weakest link but what can we do? Here are some tips for a realistic approach to training employees.

1. **Awareness Programs** – these include basic training combined with ongoing awareness campaigns. Successful awareness campaigns combine education, communications, cheerleading, entertainment, and perhaps some incentives.

2. **Leadership** – The CISO may be responsible for cybersecurity, but he/she should not be the face of end-user awareness programs. Instead, the CEO and business managers must take the lead and make it a goal to communicate that online behavior and cybersecurity awareness is as important as any other work-related task, such as meeting deadlines, attendance, or treating people with respect. This should be communicated consistently so that it drills into the employee's minds and is a part of their corporate culture.

3. **Notifying end users of policy violations with clear reasoning** – Some security tools frustrate employees by blocking their actions without further explanation. In many cases, this is frustrating to employees who may not understand why they were prevented from doing their jobs. Rather than blindly enforcing policies, progressive companies also use electronic notifications to educate employees as to why their actions were blocked in the first place. For example, an employee may not realize that the file they were trying to email contained healthcare records or other regulated data. A powerful change would be to provide a simple explanation in the form of a

pop-up or something similar to explain the blockage or violation. CISOs have reported that with this simple explanation, the volume of policy violations can decrease up to 90%.

4. **Proactive Spear Phishing** – This tactic involves sending bogus but authentic-looking emails to internal employees to see if they actively click on links, install software, or open attachments. On average, about one-third to half of the employees will do so. This can be used as a "teachable moment" by sending the employee a notification of what just happened and remind them of good online behaviors. Evidence indicates that internal spear phishing can lead to improvements in user education and behavior.

5. **End-User Feedback** – The security team needs to keep employees up to date on how they are doing by giving them feedback. How are employees suppose to improve and get better if they don't know how they are doing or they don't have a baseline to go off of? Measurable improvements should come with some type of "Yay! Wow! Congratulations" message from the CEO or a token reward from the company like a free lunch or points towards redeemable items or anything your company wants to come up with that makes it fun and rewarding for your employees. Remember your employees are the people and they are your assets and you must take care of them well.

WHAT CYBER SECURITY POLICIES SHOULD INCLUDE:

Your policy for end users should include:

- It's purpose
- Program-Level and Issue-Specific Policies
- The responsibilities of the end-users
- Compliance standards that spell out what the consequences will be for not following the policy, regardless of whether or not an attack is successful.

In order to give your policy the best chance of succeeding it needs to be:

- Implemented
- Enforced
- Free of unreasonably constraints on employee productivity
- Concise and easy to understand
- End users should constantly be reminded about potential threats and kept up to date with constant training and education on a periodic basis with measurable results.

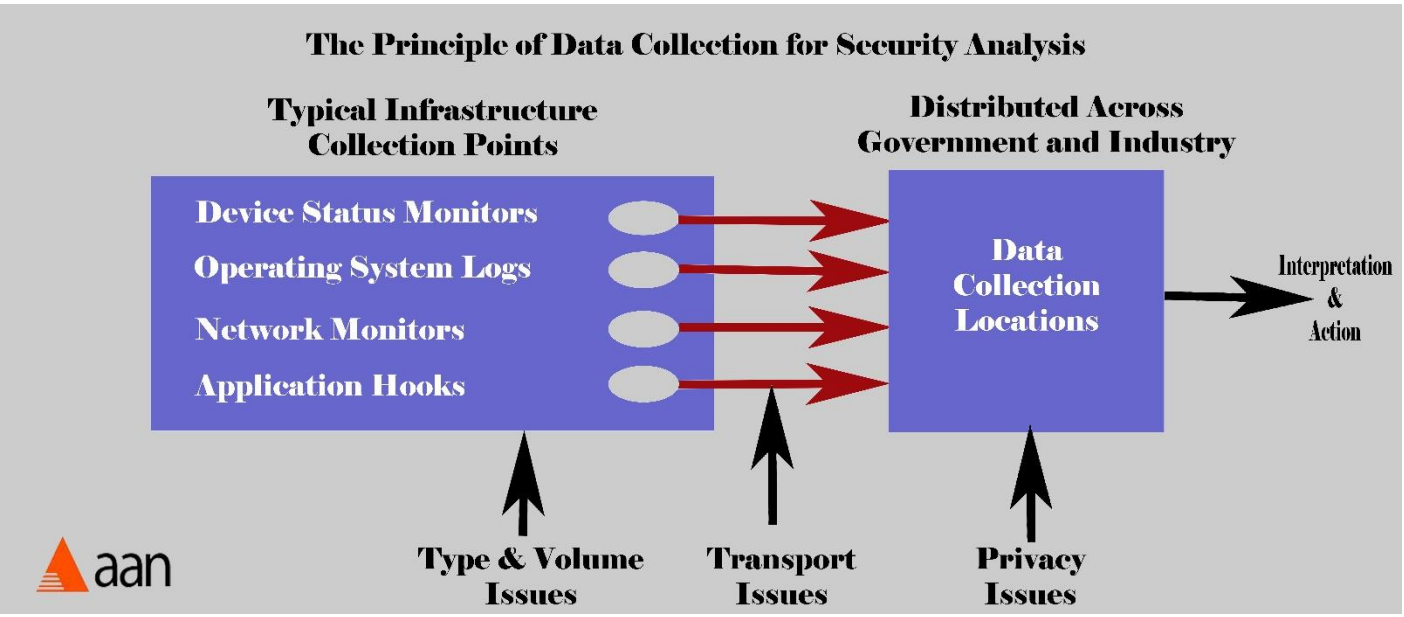
THE PRINCIPLE OF DATA COLLECTION FOR SECURITY ANALYSIS

The principle of collection involves automated gathering of system-related information to enable security analysis. Such collection is usually done in real time and involves probes or hooks in applications, system software, network elements, or hardware devices that gather information of interest. The use of audit trails in small-scale computer security is an example of a long-standing collection practice that introduces very little controversy among experts as to its utility. Security devices such as firewalls produce log files, and systems purported to have some degree of security usefulness will also generate an audit trail output.

The practice is so common that a new type of product, called a security information management system (SIMS), has been developed to process all this data.

The primary operational challenge in setting up the right type of collection process for computers and networks has been two-fold: First, decisions must be made about what types of information are to be collected. If this decision is made correctly, then the information collected should correspond to exactly the type of data required for security analysis, and nothing else. Second, decisions must be made about how much information is actually collected. This might involve the use of existing system functions, such as enabling the automatic generation of statistics on a router; or it could involve the introduction of some new type of function that deliberately gathers the desired information. Once these considerations are handled, appropriate mechanisms for collecting data from infrastructures can be embedded into the security architecture.

Figure 1.4: The Principle of Data Collection for Security Analysis



CHAPTER 2: CYBER ATTACKS & THEIR CHARACTERISTICS

- What is the meaning of Cyberattack?
- What is cybercrime?
- The changing face of cybercriminals
- The lifecycle of an advanced attack
    - Infection
    - Persistence
    - Communication
    - Command and control
- Recognizing key characteristics of advanced Malware
- Threats to the enterprise
    - Targeted intrusions
    - DDoS and Botnets

What is the meaning of Cyber Attack?

A cyber attack is an attack launched from one computer or more computers against another computer or network or multiple computers. Cyber attacks are carried out through digital means and can be launched from any part of the globe and can at once hit multiple targets.

Cyber attacks can be broadly classified into two categories -

- An attack where the objective is to disable or knock out a target computer
- An attack where the objective is to gain access to some sensitive information from a computer and in turn admin privileges to that system

Some of the techniques used by attackers to achieve their objective are -

- ***Malware (malicious software)*** - it is downloaded onto a target computer that can do anything from steal data to encrypt files and demand ransom
- ***Phishing*** - these are emails that are crafted to trick victims into revealing passwords or taking some other harmful action
- ***Denial of Service attacks*** - a technique in which a web server is overwhelmed with bogus traffic
- ***Man in the middle attacks*** - a technique in which the target computer is fooled into joining a compromised network

Given below is a list of some of the large recent cyber attacks that have taken place -

1. ***WannaCry*** - a ransomware attack that took place in May 2017, wherein the ransomware took over infected computers and encrypted the hard drives. The hard drives could be unlocked only on making payment through bitcoins.
2. ***NotPetya***- a ransomware that started circulating through a phishing spam in 2016. It encrypted the

master boot record of infected machines, making it extremely difficult for users to get access to their files.

3. ***Ethereum*** - a Bitcoin-style cryptocurrency, and $7.4 million in Ether was stolen from the Ethereum app platform in a manner of minutes in July. Then, just weeks later came a $32 million heist.
4. ***GitHub***- the version control hosting service GitHub was hit with a massive denial of service attack, with 1.35 TB per second of traffic hitting the popular site.

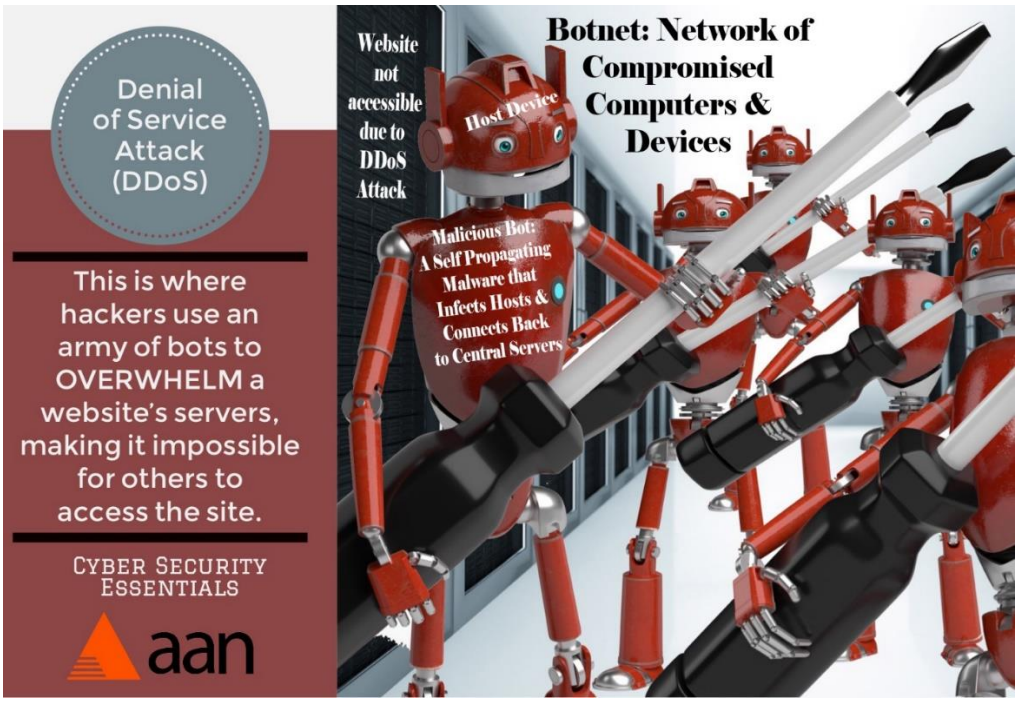
What is Cyber Crime?

Cybercrime is a computer crime, carried out with the use of digital tools either to steal some information from another system or to carry out illegal activities. Whatever you call them, cybercriminals frequently use the same kinds of attacks. It's the cybersecurity expert's job to become familiar with these attacks.

Listed Below are *Some Types of Cyber Crime* -

- **Hacking**- an act committed by an intruder wherein they access your system illegally without permission. Hackers are generally expert software developers who understand the intricacies of a computer system and misuse their knowledge for hacking. Some of the techniques used by hackers are-
    - **SQL Injections**- a technique which allows hackers to exploit the security vulnerabilities of the software that runs a website. It plays on a weakly protected SQL database
    - **Theft of FTP passwords**- a technique used by hackers wherein they target systems where the webmaster stores a website's login information on a poorly protected PC.
    - **Cross-site scripting**- the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed.
- **Virus Dissemination**- virus is a computer program that attaches itself or infects to some files in a system and it can spread easily on a network. A computer virus is capable of disrupting operations on the computer system and also can affect data.
- **Logic Bombs**- a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event.
- **Denial-of-Service Attack (DDoS)** – Another common cyber attack is a distributed denial of service attack or DDoS. Hackers use an army of bots to overwhelm a website's servers, making it impossible for others to access the site. The attacker denies service of a particular application to the user. The network is flooded with huge amount of traffic thereby ensuring server overload and non-availability of the service.

Figure 2.1: Denial of Service Attack (DDoS)



- **Spoofing and Phishing-** a technique used to extract sensitive information like credit card details, through email spoofing. Spoofing and phishing are both ways for criminals to obtain sensitive information such as usernames, passwords, and credit card information. Both of these methods trick users by making a request for information to look like it's from a safe source that the victim recognizes.

  One of the most common cyber attacks targeting regular individuals is email phishing. Hackers send an email that looks like it came from a bank, credit card company, or other business, asking for the individual's personal information.
- **E-mail bombing and spamming**- an attacker sends large volumes of email to the target e-mail address. If multiple accounts of a mail server is targeted, it can give rise to denial-of-service situation.
- **Data Diddling** - unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track.
- **Horse** – A common kind of attack is the Trojan Horse, which is a malicious, or very harmful program that appears to be harmless. This tricks the user into downloading and running the program.
- **Clickjacking** – Clickjacking hides viruses and other malware beneath clickable content on trusted websites. When a user clicks on this content, they unknowingly download a harmful program.

What are Cyber Security Experts Concerned About?

Cybersecurity experts are concerned with a system's vulnerabilities, or weaknesses. One of the most important tasks is to secure systems against exploitable vulnerabilities. An exploitable vulnerability is a security flaw for which at least one working attack exists. These attacks are known as "exploits". Cyber attacks can occur for a number of different reasons. Some attackers are thrill seekers.

What is the alibi behind cybersecurity threats like hacking, phishing, spoofing, clickjacking and more?

While some criminals use hacking for financial gain, some hackers use it to promote a political agenda, or plan, or some do it for the thrill of things. These hackers are known as hacktivist, which is a combination of the words "hacker" and "activist". Some hacktivists feel it's their job to obtain and release information about social, economic, and political issues that those in power may not want the public to have access to. Perhaps the most famous hacktivist group is Anonymous.

Some are criminals looking for financial gain. Others are activists in search of evidence that could get people in trouble.

Most people are familiar with the term "hacker". The popular meaning of the word "hacker" is someone who breaks into computer systems for criminal purposes. In the computer community, a hacker is anyone who is a highly skilled computer expert. Among members of this community, a hacker who performs illegal break-ins is known as a "cracker"

The Changing Face of Cyber Criminals

Cybercriminals have evolved drastically. It's no more a smart college kid sitting in their college dormitory trying to hack into systems for fun. Today cybercriminals are motivated by a huge financial gain and are sponsored by nation-states, criminal organizations and radical political groups. Today's cyber attacker's profile looks something like this-

- Has far more resources available to facilitate an attack
- Has greater technical depth and focus
- Is well funded
- Is better organized

The new-age cybercriminal knows exactly what to do with the stolen information. They are aware of how to exploit it. Nation-states and criminal organization have access to lots of financial resources in comparison to individuals. You can come even across office setups that look like any other regular office carrying out their business, whereas in fact it is filled with cybercriminals carrying out their client's bidding.

In old Western movies, it was common for the good guys to wear white hats and the bad guys to wear black hats. These visual aids allow viewers to identify the heroes and the villains on sight. Over time, "white hat" and "black hat" have become standard terms for good guys and bad guys.

Types of Hackers -

- **Script Kiddies** - these hackers are typically unsophisticated who use copied scripts or code to launch an attack. These attacks are generally denial of service attacks.
- **Green Hat** - these hackers seek to become full-blown expert hackers or crackers
- **Blue Hat**- these hackers are typically ones that are out to seek revenge and will do so through any means. They strike through malicious code that can shut down networks.
- **White Hat**- these are ethical hackers who have technical degrees and offer their services towards ethical hacking. They look out for security vulnerabilities and in turn work towards creating a safe

environment

- **Black Hat** - these hackers also known as crackers write their own code or use other code to steal data to sell for profit
- **Gray Hat** - most of the hackers fall in this category, wherein they are more about hunt and chase than the rewards. They break the law sometimes, but do not have bad intentions like black hats.
- **Red Hat** - these hackers hunt down black hats rather than reporting them. Red Hats are tech-savvy hackers and it's usually a test of skill and talent between them and black hats.

When it comes to cybersecurity, there are white-hat hackers and black-hat hackers. White-hat hackers are hackers who specialize in testing a computer network's vulnerabilities through the usual kinds of attacks used by criminal hackers, or black-hat hackers. Sometimes a company will employ two groups of white-hat hackers. One group, the red team, will attack a system. The other group, the blue team, will be responsible for defending the system.

The Lifecycle of an Advanced Attack

Cyberattack strategies have evolved drastically over the years. Today they are carefully planned and executed to cause maximum damage. A cyber attack today is a multi-step process that blends exploits, malware, and evasion into an ongoing coordinated network attack.

Key components of the advanced attack strategy include

- Infection
- Persistence
- Communication
- Command and Control

Infection

This is the initial stage that is the social aspect wherein users are lured into a trap, which leads to a bigger cyberattack. This stage usually involves trapping the user by sending them a malicious link or luring them to a social networking site or redirecting them to a malicious website by using an infected image.

With shell access, it is possible for the attacker to deliver almost any kind of payload. The first step is to exploit the target and deliver the malware in the background either through the application or a connection that is already open. This is one of the most common mechanisms used today to deliver malware.

Infection relies heavily on hiding itself from traditional security solutions. Another common way to avoid security is to infect the user over a connection that security can't see into, such as an encrypted channel.

The rampant trend today is that you no longer need just an email to target a particular network. It can be infected with just the use of a link. That's why we need to be more careful of using social media platforms, micro-blogging sites, message boards, which have all become platforms that are exploited by attackers.

Persistence

Once the network is infected, next it depends on how long it can persist/sustain. To persist an attack, rootkits and boot kits are used. A rootkit is a kind of malware that provide privileged access to a computer. A bootkit is a kernel-mode variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption.

Backdoors allow the attacker to get past normal authentication procedures to gain access to a compromised system. Backdoors are installed for use, in case other malware is detected and removed from the system. Anti-AV malware may be installed to disable any legitimately installed antivirus software on the compromised machine, thereby preventing automatic detection and removal of malware that is subsequently installed by the attacker.

Communication
For an Advanced Persistent Threat to be successful, communication between infected systems is essential which an attacker should be able to carry out. Attack communication should be stealthy and done in a manner so that it does not raise any unwanted suspicion on the network. Such traffic is usually hidden through some of the techniques listed below.

- Encryption - with Secure Sockets Layer (SSL), Secure Shell (SSH) or some other custom application.
- Circumvention - via proxies, remote desktop access tools or by tunneling applications within other (allowed) applications or protocols.
- Port evasion using network anonymizers or port hoping to tunnel over open ports.
- Fast Flux (or Dynamic DNS) to proxy through multiple infected hosts, reroute traffic, and make it extremely difficult for forensic teams to figure out where the traffic is really going.

Command and Control
Command and control is about ensuring that the attack is controllable, manageable and updateable. This is accomplished through webmail, social media, P2P networks, blogs, and message boards. This traffic is hard to detect as it is encrypted and it makes use of backdoors and proxies.

Recognizing Key Characteristics of Advanced Malware

Some malware has the ability to mutate or can be updated to avoid detection by traditional malware signatures. Additionally, advanced malware is increasingly specialized to the point where the attacker will develop a customized piece of malware that is targeted against a specific individual or network.

Botnets are useful for understanding characteristics of advanced malware. Bots (individual infected machines) and botnets (network of bots working together) are difficult for traditional antivirus/anti-malware solutions to detect. Botnets are centrally coordinated, networked applications. All malware of the same type can work together toward a common goal, with each infected machine growing the power and value of the overall botnet.

Some characteristics include -

- ***Distributed and fault tolerant*** - a botnet can have multiple control servers distributed all over the world, with multiple backup options. Bots can even make use of other infected communication channels thereby providing them a wider access and more communication paths.
- ***Multifunctional*** - updates given by the command and control server can also change the bots' functionality completely. The multifunctional capability allows a bot to perform different tasks, like one bot can be collecting credit card numbers while the other can be sending spam.
- ***Persistent and intelligent*** - they are well suited for long-term intrusions into a network, because they are not detected easily.

Threats to the Enterprise

Considering the capabilities of botnets, including flexibility and ability to avoid defenses, they present a huge threat to enterprises. Advanced malware is virtually unlimited in terms of functionality — from sending spam to the theft of classified information and trade secrets. Since it also has multifunctional ability, it can be performing different tasks at different times making it much more dangerous.

Targeted Intrusions

Botnets are also a key component of targeted, sophisticated and ongoing attacks. These kinds of botnets, which are smaller, do not aim to attack large number of systems. Instead their focus is on specific high-value systems that can be used to further penetrate into a larger network. In these cases, the infected system can be used to gain access to a network of protected systems and hence establishing a backdoor in case the intrusion is detected.

These kinds of targeted intrusions are almost undetectable by anti-virus software. This kind of an attack poses a bigger threat to an enterprise because it almost always ends up targeting the most valuable and sensitive information belonging to an enterprise.

DDoS and Botnets

Bots can be used as part of a distributed denial-of-service attack (DDoS) overwhelming a target server or network with traffic from a large number of infected endpoints. DDoS attacks often target specific companies for personal or political reasons, or to extort payment from the target in return for stopping the DDoS attack.

A DDoS attack on an enterprise causes loss of productivity due to the downtime. The infected machines in the enterprise consume valuable resources and facilitate a criminal act unwillingly.

New Kaspersky Labs Research, notes that the financial impact of a Distributed Denial of Service (DDoS) attack continues to rise, and is now more than $120K for SMBs and more than $2M for enterprise organizations.

CHAPTER 3: DEALING WITH CYBERSECURITY THREATS

- Introducing the next-generation firewall
- Preventing infections with next-generation firewalls
    - Reduce the attack surface
    - Control advanced malware-enabling applications
    - Actively test unknown files

    - Prevent use of circumvention
    - Investigate any unknown traffic
- Safe enablement through smart policies
    - Application controls
    - User controls
    - Network controls
    - Endpoint controls
- 10 best practices for controlling APTs
- Principle of Depth: Using Multiple Security Layers

Introducing the Next-Generation Firewall

The next-generation firewall is equipped to fight against advanced malware. It provides visibility and control of all the traffic on the network irrespective of the port or evasive tactics used. It's critical to analyze all the traffic in the network or else it becomes a challenge to protect oneself from the various threats. By completely analyzing the network traffic, you will be able to control the behavior that is allowed in the corporate environment and in turn eliminate the shadows that APTs (Advanced Persistent Threats) hide. These attacks have to communicate with each other in order to sustain. By observing the communication patterns, you will be able to control cyberattacks and the threats they pose.

A next-generation firewall performs classification of network traffic based not simply on the port and protocol, but on an ongoing process of application analysis, decryption, decoding, and heuristics. The ability to pinpoint and analyze even unknown traffic is the true character of a next-generation firewall and it is this ability that will help greatly in the fight against APTs.

Cybercriminals have an innate ability to blend in with regular network traffic. The quality of your visibility into that traffic is critical. The next-generation firewall also provides a fully integrated approach to threat prevention in a unified context. This kind of integration provides a better understanding and insight into unknown threats.

Preventing Infections with the Next-Generation Firewalls

Advanced malware can be controlled by reducing attack vectors and also by not allowing bots to hide in the network. Malware traffic can easily blend in the background and hence it is important to keep check on the vectors used by malware. Security experts need to gain full control and visibility of the network traffic in order to prevent unnecessary cyberattacks from taking place.

Reduce the Attack Surface

Positive control is a technique wherein you allow only the specific applications and traffic you want into the network, instead of blocking everything. Positive control is critical to control malware attacks. Positive control drastically reduces the attack surface and in turn reduces the overall risk.

In an organization, it is not easy to extend positive control to all applications. These days with the widespread use of multiple social media platforms, and with the increase in use of personal devices at work, a proper security policy is a must. The organizational security team must consult with the appropriate stakeholders within the organization and frame a robust security policy that should clearly define the applications that employees can have access to at work.

***Key points to keep in mind to reduce attack surface are*:**

- Positive control must be enforced on all kinds of network traffic irrespective of the encryption techniques used to hide the traffic. Unnecessary or high-risk traffic must be avoided at all costs
- Policies need to be established based on the application uses and the needs of a business by deciding -
    - What applications and protocols are being used on the network?
    - What applications are required for the business and who uses them?
    - What dual-use or personal applications the company would like to allow?

Control Advanced Malware-Enabling Applications

Applications are an indispensable part of a cyber attack lifecycle. The initial infection stage is generally through an application. An application with weak security features becomes a vulnerable target for a cyber attack.

Applications have been a soft target for malware since a long time. Earlier e-mails were an easy target for cyber attackers. A malicious link sent through an email has been a favorite technique for cyber attackers. Hence, organizations have started to focus more on providing stronger email security. With emails being a strong focus for organizational security, cyber attackers have now moved on to social media platforms, which has become a widespread target.

Social networking and personal use applications are easy targets for malware infection and subsequent command and control. These applications or platforms are designed for easy information sharing. Majority of social media users are not aware of the security threats that a social platform can give rise to and make use of it with a cavalier attitude. This gives attackers an easy target for infection opportunities. Unsuspecting social media users become very soft targets in cases wherein they click suspicious links, befriend an unknown person on social media or get tricked by an impersonator on social media. Cyber attackers who exploit systems use all these techniques.

Actively Test Unknown Files

Malware and exploits are easily customizable by attackers, so that their attack does not trigger any known signatures. This flexibility is one of the key advantages that attackers make use of to get into a network without raising any suspicion. New technologies need to be integrated to keep a check on unknown files and actively monitor them.

Virtual Sandbox

This active analysis of suspicious files can be executed using a virtual sandbox. The sandbox is a virtual environment that allows you to observe how certain files behave and what they reveal in terms of threats.

Active analysis malware is to be coupled closely with the next-generation firewall so that the results can be used for enforcement.

Typical in-line enforcements include -

- Protection for newly identified unknown malware, zero-day exploits, and their variants
- Protection for malware that may use command and control server or infrastructure
- Protection for threats that use related domains and URLs

Points to keep in mind to control applications -

- Block use of bad applications that allow P2P file sharing
- Application usage and access to be limited to the one who really needs it
- Disabling specific features in applications such as file transfers which is a potential risk
- Prevent automatic download of files without the user's knowledge from unknown websites
- Decrypt SSL traffic selectively

Prevent use of circumvention -

A set of applications is designed in such a way that they evade traditional network security.

Applications like the following list can evade network security:

- remote desktop technologies,
- proxies
- purpose-built circumventing applications

The risks posed by remote desktop technologies are -

- When a user connects to a remote PC there is no control on the user's surfing activity. The network

traffic is not being inspected by the firewall. This circumventing technique is risky and the results are tunneled back to the user's system within the organization.
- Remote desktop technologies allow an unauthorized user to gain full access into a trusted enterprise network. This is one of the first steps of intrusion for malware.

Common applications used within an organization by unauthorized users or untrained users can also expose the application to cyber attacks.

Lastly, web proxies and encrypted tunneling applications allow users secure and anonymous communication across firewalls and other security infrastructure. These tools, apart from undetected web surfing, also allows file sharing and access, which is risky behavior that must be blocked completely.

Investigate any unknown traffic

Once an organization has regained positive control and has the ability to identify and classify authorized traffic on the network, it is important to monitor unknown traffic. Malware and APT traffic often appear as 'unknown' traffic.

A next-generation firewall has the ability to inspect unknown traffic. If unknown traffic is being detected by the same source repeatedly, it is necessary to determine the source and if the traffic is malware or harmful traffic.

The security team can also analyze where the traffic is going -

- Does it go out to known malicious websites or to social networking sites?
- Does it transmit on a regular schedule?
- Does someone attempt to download or upload files to an unknown URL?

If you notice any of the aforementioned behavior, this highly indicates the presence of a bot. With the use of the next-generation firewall, the unknown network traffic can be identified and analyzed and hence preventing damage to the system. The next-generation firewall not only analyzes unknown traffic, it can also identify and analyze unknown files.

Systematic management of unknown traffic can be done by-

- Enforcing a policy on the firewall to block all unknown traffic or allow it and inspect it further
- Determining what internal applications exist on the network, and either applying an application override or creating a custom signature
- Use sandbox to analyze unknown files
- Use packet captures to analyze unknown traffic
- Use botnet reports or other forensic tool to analyze which kind of traffic is a threat

Safe enablement through smart policies

The purpose of an enterprise security policy is to protect an organization from advanced threats. However, no matter how strong or secure your policies might be, security breaches are bound to happen. Your security policy must help your organization control malware and reduce risks, while also meeting your business requirements.

Four Major Stakeholders in the Enterprise Network

It must play a key role in designing these smart security policies that will mitigate risks and protect an organization's users. Governance and management work best if they are based on a set of smart corporate policies that are developed by the four major stakeholders in the enterprise network: IT, HR, executive management, and the users.

Application Controls

It is essential to have an understanding of user behavior and also the applications they are making use of. Social media applications are being used rampantly by users within and outside the organization. Even though users are well versed with social media platform usage, they are oblivious to the security threats they pose. As a result, it's vital to match users' needs with the most appropriate applications and features, while also educating users about the implicit risks of those applications and features.

Application Enablement

This is basically restricting the use of unnecessary risky applications and also closely monitoring the allowed applications for usage and any threats that might arise from them. Application controls should be part of the overarching corporate security policy.

Again, there may be some applications which fall in an in-between category of not being too good or too bad, but still holds business value for people to use it. Such applications must be dealt with care and can be allowed but constrained to only allow needed features while blocking higher risk features.

User Controls

Most companies have some type of application usage policy, outlining which applications are allowed and which are prohibited. Every employee is expected to understand the contents of this application usage policy and the ramifications of not complying with it, but there are a number of unanswered questions, including

- Given the ever-growing numbers and types of applications, how will an employee know which applications are allowed and which are prohibited?
- How is the list of unapproved applications updated, and who ensures employees know the list has changed?
- What constitutes a policy violation?
- What are the ramifications of policy violations — a reprimand or termination of employment?

The development of policy guidelines is often a challenging and polarizing process. Determining what should be allowed and what should be prohibited while balancing risk and reward elicits strong opinions from all the major stakeholders.

Further complicating the process is the fact that new applications and technologies are often adopted within an organization long before appropriate policies governing their safe and appropriate use are ever considered or developed.

Network Controls

Given that advanced threats most often use the network for infection and ongoing command and control, the network is an obvious and critical policy-enforcement point. With application-enablement policies in place, IT can shift its attention to inspecting the content of allowed traffic. This inspection often includes looking at traffic for known malware, command-and-control patterns, exploits, dangerous URLs, and dangerous or risky file types.

The goal should be to create written policies that reflect the policies' intentions just like someone might describe them orally

SSL

SSL stands for secure sockets layer and ensures that all data transmitted between the web server and browser remains encrypted. SSL is another key component of network policy to create the absolute need to retain visibility into the traffic content. SSL is increasingly used to secure traffic destined for the Internet. Although this may provide privacy for that particular session, if IT lacks the ability to look inside the SSL tunnel, SSL can also provide an opaque tunnel within which malware can be introduced into the network environment. For this reason, it is important to establish SSL decryption policies that can be enforced selectively by application and URL category.

Endpoint Controls

Endpoint policies must incorporate ways of ensuring that antivirus and various host-based security solutions are properly installed and up to date. The end user's machine is the most critical point for security policy enforcement. Endpoint solutions must be kept up to date and must be monitored regularly.

Host operating systems also need to be updated regularly. Several malware infections begin with a remote exploit that target a known vulnerability within the operating system. Reducing the attack surface for an enterprise includes keeping all these components updated and regularly audited.

Desktop Controls

Desktop controls are a key piece to the safe enablement of applications in the enterprise. Desktop controls need to be given careful consideration as they directly impact employee productivity. Desktop lockdown is not a practical solution, as it is not feasible to restrict employees from installing their own applications. Desktop controls can complement documented employee policies as a means to safely enable Web 2.0 applications.

10 BEST PRACTICES FOR CONTROLLING APTs

1. **Ensure visibility into all traffic -** You can ensure visibility into all traffic on the network by:
   a. **Accurately classifying all traffic** - A next-generation firewall uses protocol decoders to fully analyze the application layer and to accurately classify the application and traffic.
   b. **Extending visibility beyond the perimeter** - protect high-value targets and remote users.

2. **Restrict high-risk applications** - The number of applications being used and the variety of applications have drastically increased over the years. With this also comes high amount of risk to the enterprise systems. Most applications are designed for easy use, easy sharing, and easy interaction. Security is almost always an afterthought, and it is up to IT security teams to control these risks.

   a. Some tips on how an organization can control the risk brought about by high-risk applications -

   - Block (or limit) P2P applications
   - Block unwanted applications that can tunnel other applications
   - Block applications known to be used by malware
   - Block anonymizers (such as Tor)
   - Block encrypted tunnel applications
   - Limit use of approved proxies to authorized users with a legitimate business need
   - Limit use of remote desktop protocols and applications to authorized users with a legitimate business need

3. **Selectively decrypt and inspect SSL traffic -** Enterprises can control SSL traffic with:

   a. **Decrypt policies** that allow decryption and inspection of the following SSL traffic:
      - Social networking
      - Web-based e-mail
      - Instant messaging
      - Message boards
      - Microblogging
      - Gaming sites

   b. **Do-not-decrypt policies** that protect the confidentiality and integrity of the following SSL traffic:

- Healthcare applications, information, and sites
- Financial applications, data, and sites
- Secure channels

4. **Sandbox unknown files -** IT security teams should have the ability to create protections on demand when new malware or exploits are identified and distribute these custom protections to all of the organization's network gateways in order to protect against unknown threats. It's not enough to simply put a sandbox into your lab. You must build up the ability to quickly and centrally determine whether a given file has already been analyzed, and then quickly deliver protections to all ingress or egress points when a malicious file is detected.

5. **Block URLs that are known to host malware and exploits -** IT security teams must be able to update URL classifications based on malware and exploits that may have been identified through sandboxing. An important benefit of a sandbox is the ability to see how and where the threat came from, and where it connects back to. This will allow security teams to immediately update the lists of dangerous URLs, based on actual threats observed in the network.

6. **Enforce drive-by-download protection -** Enterprises must enforce drive-by-download protection to prevent infections by:

   a. Detecting downloads in the background, even unknown exploits and malware
   b. Automatically reporting drive-by-downloads to the user and either blocking the download or requiring the user to acknowledge and permit the download
   c. Training users not to just click "OK" or "Accept" but to read and understand pop-up warnings from their network firewall

7. **Block known exploits and malware -** IT organizations commonly disable many known vulnerability signatures and features (such as real-time vulnerability scanning) in intrusion prevention systems or anti-malware software for performance reasons. The single unified threat engine in a true next-generation firewall is designed to process high volumes of network traffic in real-time to detect all threats, without sacrificing performance or reliability.

8. **Limit traffic for common applications to default ports -** Certain ports practically have to be open on a firewall for an enterprise network to function. Attackers take advantage of this requirement with malware that regularly communicates on ports that are almost always open by default. Legacy port-based firewalls simply allow traffic across an open port and assume that it is the default application or protocol for that port. A next-generation firewall compares the traffic to application signatures in order to accurately identify the application or protocol and allows you to set policies that permit only the default application on a common port and block everything else.

9. **Evaluate network and application events in context**

   a. Develop context-based visibility with accurate information about applications, signatures, sources, and behaviors
   b. Correlate events by user and application including -
      - Known malware
      - Known exploits
      - Phone-home detection

- Download history
- URL categories

10. **Investigate unknowns -** A true next-generation firewall accurately classifies all known traffic and allows you to create customized classifications for any remaining unknowns, such as internal or custom-developed applications.

In addition to unknown traffic, you should investigate

a. **Unknown or unclassified URLs** - Unknown or recently registered URLs are significant because malware and bot-herders regularly rotate between URLs that are used for command and control to impede discovery and take-down efforts. Unknown traffic going to unknown URL categories should be treated as highly suspicious.

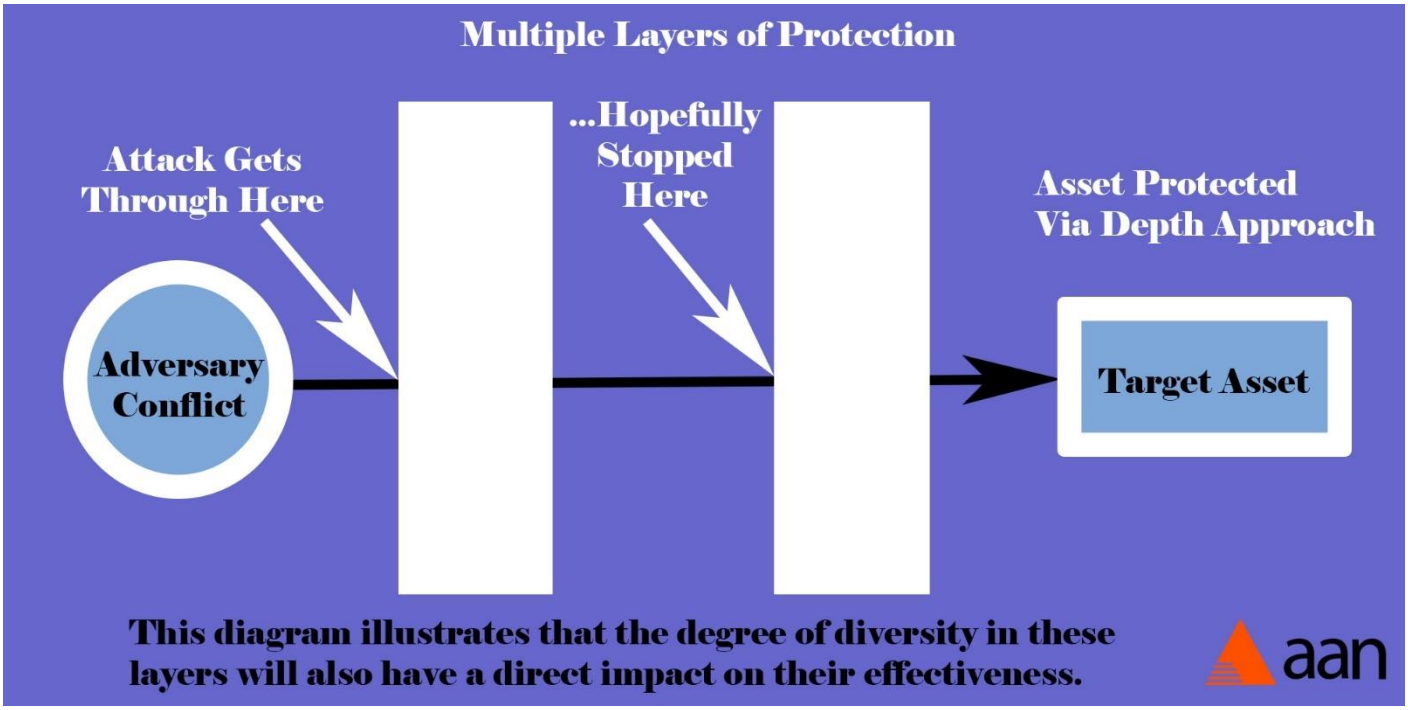
b. **Unknown encryption -** Customized encryption is often used by malware to hide their communications. Use the capabilities of a true next-generation firewall to inspect encrypted traffic and to ensure that all traffic on the network has a known, legitimate purpose.

PRINCIPLE OF DEPTH: Using MULTIPLE SECURITY LAYERS

The principle of depth involves the use of multiple security layers of protection for digital assets. These layers protect assets from both internal and external attacks via the familiar "defense in depth" approach; that is, multiple layers reduce the risk of attack by increasing the chances that at least one layer will be effective. This should appear to be a somewhat sketchy situation, however, from the perspective of traditional engineering. Civil engineers, for example, would never be comfortable designing a structure with multiple flawed supports in the hopes that one of them will hold the load. Unfortunately, cybersecurity experts have no choice but to rely on this flawed notion, perhaps highlighting the relative immaturity of security as an engineering discipline.

One hint as to why depth is such an important requirement is that infrastructure components are currently controlled by software, and everyone knows that the current state of software engineering is sometimes abysmally bad. Compared to other types of engineering, software stands out as the only field that accepts the creation of knowingly flawed products as acceptable. The result is that all non-trivial software has exploitable vulnerabilities, so the idea that one should create multiple layers of security defense is unavoidable and expected.

Figure 3.1: Multiple Layers of Protection



Multiple Layers of Protection Diagram

It is recommended that a combination of functional and procedural controls be included to maximize the usefulness of defense layers. For example, a common first layer of defense is to install an access control mechanism for the admission of devices to the local area network (LAN) and could involve router controls in a small network or firewall access rules in an enterprise network.

CHAPTER 4: ADDITIONAL READING & CASE STUDIES

Biggest Breach, Massive Security Breach at Sony, How Mphasis safeguards its Information, Uber Suffered from Security Breach, Insider Threats in Cyber Security: What can users Do to Protect Themselves, Target-Opening of Email which has threats

BIGGEST BREACH OVERVIEW CASES

The number of large data breaches, or break-ins increases every year. Private corporations, academic, and financial institutions, and governments have all been victims of cyber attacks. Each new hack reveals an exploit that cybersecurity experts have to deal with.

One of the largest data breaches to date was also one of the earliest. Between 2005 and 2012, a group of Russian and Ukrainian hackers attacked a number of banks and corporations, including 7-Eleven, JetBlue, and JCPenney. The hackers ended up stealing 160 million credit and debit card numbers and breached 800,000 bank accounts. In 2014, JPMorgan Chase and Co., the largest bank in the United States, was the victim of a cyberattack that exposed the data of more than half of all households in the country.

Cybercriminals like to attack large companies such as Amazon and Walmart. Companies like this are large and convenient so they are the perfect targets for someone looking to steal the personal and financial data of millions of people all at once.

Target, Home Depot, and eBay have all been targeted by cybercriminals since 2013. The Target and Home Depot attacks resulted in the exposure of millions of debit and credit card numbers.

In the last few years, some of the largest companies in the world have been victims of cyber attacks and data breaches. In 2014, eBay announced they had been hacked and the names, addresses, and passwords of around 145 million users had been exposed. Fortunately, eBay kept financial information on a different server, preventing the hackers from accessing this data. In December 2016, Yahoo announced that more than 1 billion user accounts had been hacked three years earlier. It can take a long time for companies to realize they've been hacked, so that is why it is important to keep up-to-date with the latest security threats and to have a keen eye on suspicious trends in your network.

In 2011 and 2014, it wasn't just fun and games when Sony's PlayStation Network (PSN) was the repeat victim of two cyber attacks that affected millions of users. After discovering the breach in 2011, Sony shut down the gaming network for three weeks. Unfortunately, in the end, the hackers were able to steal the personal and financial data of 77 million users. Three years later, in December 2014, Sony's PSN was the victim of another cyber attack. This time it was a DDoS attack that prevented users from accessing the network for several days.

In 2015, a department of the U.S. government was hacked. Up to 14 million current and former federal employees had their private information exposed. The U.S. government was subject to about 61,000 cybersecurity breaches in 2014, which is proof that no system is truly safe.

A CLOSER LOOK AT THE MASSIVE SECURITY BREACH AT SONY

In late April of 2011, Sony, Inc. shut down its online PlayStation Network (PSN) in response to a data security breach. Over seventy-seven million users use the network in countries across the globe, and it is an integral part of Sony's video game system. For almost a week, Sony failed to inform PSN users as to the reason for the network shutdown. A message was subsequently posted on Sony's website stating that the company suspected unidentified individuals had stolen PSN users' personal information. Stolen data included names, home addresses, e-mail addresses, birth dates, network passwords and login information.

A later e-mail sent to all PSN users revealed that Sony suspected credit card information had also been obtained. Sony kept the PSN down for almost a month until the network resumed on May 14, 2011. Sony was highly criticized for waiting a week to inform customers of the reason for the network shutdown. Some observers took the opportunity to draw unfavorable comparisons to some of Sony's biggest competitors such as Apple and Microsoft. After another attack in June, one security expert even referred to Sony as the whipping boy of the computer underground. The data breach also prompted members of Congress to call for private and public reforms in standards for protecting online personal information. With mounting criticism over the lack of data security and poor financial performance, Sony cut its Chairman's salary and bonus by 15 percent.

According to one observer, Sony's exposure as a result of the breach could reach into the tens of billions of dollars. Costs include an identity theft protection policy for PSN users and an ongoing electronic forensics exam and investigation. Sony also faces mounting liability from class action lawsuits accusing Sony of negligence and breach of privacy. With such extremely high costs, Sony is understandably seeking coverage from its insurers. With at least one insurer, Sony has faced substantial challenges in seeking coverage for many of its losses.

Zurich American Insurance Company (Zurich) petitioned a New York state court to find that Zurich does not have a duty to defend Sony in the increasing number of lawsuits filed against Sony in the wake of the breach. Zurich also joined other Sony insurers in the suit so that the court can clarify their respective responsibilities. The lawsuit claims Sony has a commercial general liability (CGL) policy with Zurich that does not cover cyber-related third-party claims.

The challenges Sony faces in seeking coverage for cyber-related losses are a telling sign of the new landscape of cyber-related liability as it relates to insurance coverage. Sony will most likely have a difficult time getting coverage under its CGL policy for most expenses associated with the data breach. Companies seeking to protect against cyber risks must now seek cyber risk-related insurance policies, which have become increasingly available over the past decade.

HOW MPHASIS SAFEGUARDS ITS INFORMATION

Fast-growing IT services businesses cannot afford network failures or security breaches. This is especially true for Mphasis, which services customers in financial services, healthcare, communications, transportation, consumer and retail, and governments around the globe.

For the comprehensive protection of information and assets, Mphasis wanted to provide accurate threat detection and response for the assets deployed in centers that cater to their key clients. In addition to threat management, MphasiS wanted to eliminate manual log examinations, which were burdensome and time consuming for the security staff.

"The protection of information and assets is crucial to our business and we need to ensure day-zero threat protection. We also want to offer manageable access options for our clients to access the networks," said Surajit Sarkhel, Associate Leader-Global Information Security, MphasiS.

Network solution

After a series of detailed discussions and evaluations with the MphasiS team, Cisco recommended a solution that included the deployment of the Cisco IPS, Cisco ASA, Cisco Security Manager products, and Cisco Security Monitoring Analysis and Response System (MARS). Cisco Security MARS appliances efficiently aggregate and synthesize massive amounts of network and security data and use sophisticated event correlation and validation intelligence to help administrators more effectively identify and respond to threats. The solution also serves as a central repository for all auditing and compliance information.

The Cisco IPS provides accurate and comprehensive threat detection and improved response with signature and network anomaly detection, assuring greater detection of known and unknown threats.

Business results

Today, MphasiS, its global delivery centers, customers, and partners are benefiting from the state-of-the-art business network and network defenses. Commenting on the business results Sarkhel said, "With our assets and information protected now, we have noticed an increase in workforce productivity and efficiency as less manual intervention is required. We are also finding it easier to meet our audit and compliance requirements".

Commenting on the engagement with MphasiS, Mahesh Gupta, Business Development Manager for Security, Cisco India and SAARC said, "With the increased security and availability in the network we believe there will be significant reduction in downtime due to the comprehensive threat detection and response. This in turn will improve employee efficiency and customer service engagements all leading to a competitive advantage in the market."

INSIDER THREATS IN CYBER SECURITY: WHAT CAN USERS DO TO PROTECT THEMSELVES

There is a high probability that either a malicious insider is going to intentionally exploit their access to your data, or a negligent worker is going to inadvertently expose it. Although you can't completely eliminate the risk posed by insider threats in cybersecurity, you can reduce the chances of a breach, and the potential damage an insider can cause if you're willing to make security a priority.

Threat Landscape: Where Insider Threats Come From

Security technology continues to advance to combat new hacking threats and techniques, but human behavior changes much more slowly. The biggest threat isn't a misguided genius exploiting a cutting-edge attack vector, it's someone in your organization making a mistake.

What Exactly is an Insider Threat?

The term "insider threat" is often used to refer to malicious insiders willfully stealing, damaging or exposing internal data or systems, but employees motivated by grievances or profit are only one small part of the total threat. Companies face a much more serious threat from workers inadvertently damaging cybersecurity or disclosing data. In some cases, a worker's action might comprise the entire breach for example, an employee could send a confidential file to the wrong client or lose a flash drive with sensitive information in a public place.

Unsecured Software: The First Major Security Threat

We've said it before, but it bears repeating that most hackers are motivated by profit, not challenge. In most cases, they behave like any professional thief would as they look for poorly guarded, valuable property, take the easiest way in they can find, and try to cover their tracks when they're done.

Many companies hire IT staff for development, but then force them to do double duty as system admins. They may be overburdened and not have time to keep up with the latest patches, or not have expertise in systems administration. Other organizations use legacy software that doesn't support advanced security features, such as encryption (hey, if it happened to the OPM — an organization that stores extensive background data on federal employees — it can happen to anyone).

Having a mobile workforce outside of a traditional office setting has a lot of advantages, but security isn't one of them. It's much harder to secure mobile devices scattered around the world, than it is to secure a row of office computers on a company network.

Breaching Security on Personal Devices

There are a huge number of ways employees can breach security on their personal devices, including:

- Downloading malware that gives hackers control over the device
- Having hackers spy on their Wi-Fi

- Losing their devices, or having them stolen
- Failing to adhere to the company whitelist or technology use guidelines

They may also wish to restrict what information can be accessed outside of the office, requiring employees to use the organization's secure network to access the most sensitive data.

Bad Access Practices: Setting Security Standards

No matter how many times you tell them, people are going to mess up password safety. One recent survey found that 73% of online accounts use duplicate passwords, and 47% of users haven't changed their passwords in five years or more. Add to this the prevalence of easily hacked passwords like "123456," "qwerty," and the ever-cringeworthy "password," and you have a recipe for disaster. If an employee shares one easily-guessed password across their accounts, a hacker will be able to get access to everything — including company assets — by hacking a single account.

Plenty of other bad access practices erode security too, including:

- Storing passwords in browsers on shared or public computers
- Failing to clear the browser cache after using public computers
- Leaving computers logged in and unsupervised
- Jumping online on unsecured Wi-Fi
- Saving passwords in unencrypted documents

You can never completely stop people from being careless, but you can mitigate the risks. Google Apps security tools allow you to enforce multi-factor authentication, and many other business productivity suites have similar functionality. With multi-factor authentication, employees will have to enter both their password and a code sent to their phone every time they want to log in.

Email Accidents: Or How a Reply All Can Sink Your Company

Email accidents happen all the time, but usually they range from harmless to mildly embarrassing. You'll auto-complete the wrong address and not notice, click "send" before you've finished recording a message or hit "reply to all" when you should really only send the message to one person.

But these sorts of mistakes can have serious consequences. One mistyped address can break compliance, or even leak a document. Send a sensitive message to a large pool of recipients instead of one particular person, and you could have compromised confidentiality already.

Virtru Email Software

Virtru Pro can keep your information secure when you send the right email and save your hide when you send the wrong one. Like Virtru Basic, it can encrypt your messages with the push of a button. But, Pro also gives you the ability to revoke emails — even after they've been read. In addition, Virtru Pro lets users set

time limits on emails, and even disable forwarding to prevent recipients from sharing sensitive messages. Virtru Pro allows you to retract emails after they've been sent and Virtru DLP can stop sensitive information from ever leaving your outbox.

Virtru admin-controllable rules can be configured to protect your whole organization in a variety of ways, including:

- Forcing encryption on sensitive emails
- Stripping attachments sent to addresses outside the organization
- Warning employees who are about to email sensitive information, or
- Forwarding copies of certain emails to an admin

The warning messages also help train employees in compliance rules, decreasing the likelihood of future compliance violations while preventing immediate breaches.

Malicious Insiders

There will always be insider threats in cybersecurity, because you can't keep information 100% safe from the people you give it to. Malicious insiders in particular are always going to be a risk, because they've already past your defenses. They have sensitive data already in their hands, and they know your weaknesses, which can help them steal even more valuable assets.

A Maginot Line approach to data protection does next to nothing to mitigate malicious insider threats in cybersecurity. In fact, it can encourage the sort of lax internal security that enables internal breaches.

In addition, organizations need to keep detailed logs, recording each user's access, and monitor them for unusual or suspicious activity. If someone starts downloading lots of information, or sending lots of traffic out of the organization, your security team can investigate it, or even close that account until they can make sure the activity doesn't represent a breach.

Finally, you need to make security part of your organizational culture. The only hope of overcoming these tendencies is making security a priority across your organization.

UBER SUFFERED FROM SECURITY BREACH

According to a statement by current Uber CEO Dara Khosrowshahi, the stolen data included names, email addresses and mobile phone numbers of users and drivers around the world, as well as driver's license numbers of around 600,000 drivers in the United States. The company paid the two hackers $100,000 to destroy the stolen data and to keep quiet about the hack.

Given that the hack is only now coming to light, it seems that they have kept that part of their bargain, but there's effectively no way to prove that they've actually deleted the data. They could be keeping it to repeat their ransom request at a later date, or they've might already quietly sold it or used it.

"Paying hackers to be quiet is not a common tactic. It's certainly under-represented because people generally aren't going to tell the world that they're doing it," notes Vincent Weafer, VP of Labs, McAfee.

"But, if we look at ransomware, a more common example of people paying criminals, we know that there's a high percentage of cases where paying does not result in data being restored. You're essentially relying on the integrity of criminals, and the wisdom or value of that is obviously debatable."

How did the hackers manage to get their hands on the data?

According to Bloomberg, the attackers accessed an insecure private Github repository used by Uber software engineers, scoured the code for sensitive info, found login credentials, and used them to access data stored on a company for Amazon Web Services account.

Zohar Alon, co-founder and CEO, Dome9, says that this type of user error is inexplicable for an organization as large as Uber.

"There are tools available right now within GitHub that automatically check code for embedded access credentials such as AWS API keys. This is something that Uber, and any organization that is developing code, can and should implement whenever a software engineer checks in code to GitHub,"

Why was the breach not disclosed at the time?

Apparently, the breach happened around the time the company was negotiating with the Federal Trade Commission on a privacy settlement regarding a breach that happened in 2014 and wasn't properly disclosed. Before that, in January 2016, the New York attorney general fined Uber $20,000 for its failure to disclose that breach.

Allegedly, Uber's Chief Security Officer Joe Sullivan and his top aide were the ones who decided to pay off the hackers and Travis Kalanick, Uber's co-founder and CEO at the time. Furthermore, Kalanick was forced to resign as the CEO in June 2017 due to allegations that he failed to do anything about the sexual harassment rampant at Uber. Sullivan, a former US Federal Prosecutor who joined Uber in 2015 from Facebook, has now been fired, along with another individual "who led the response to this incident."

Uber has long had the image of a company that does not care about rules, regulations or ethics in its quest to become the most widespread ride-hailing company. With this latest revelation, current Uber CEO Khosrowshahi is trying to change it.

TARGET – OPENING OF EMAIL WHICH HAS THREATS

During Target's infamous data breach attack, Target personnel discovered the breach and notified the U.S. Justice Department by December 13th. As of December 15th, Target had a third-party forensic team in place and the attack mitigated. On December 18th, security blogger Brian Krebs broke the story publicly in a post quoting that "The sources said the breach appears to have begun on or around Black Friday 2013 -- by far the busiest shopping day the year."

Then things became interesting as Target informed about 110 million credit/debit-card wielding shoppers, who made purchases at one of the company's stores during the attack, that their personal and financial information had been compromised and that attackers pilfered 11 gigabytes of data.

Preliminary survey

We don't know for certain if or how the attackers performed preliminary reconnaissance scouting on Target's network prior to the attack, but it wouldn't have required much more than a simple internet search. Teri Radichel, a professional that provides cybersecurity assessments, pen testing, and research services through her company, 2nd Sight Lab, LLC. Teri Radichel explains in her dissertation how the attackers may have gained information about Target's infrastructure. "Reconnaissance would have revealed a detailed case study on the Microsoft website describing how Target uses Microsoft virtualization software, centralized name resolution, and Microsoft System Center Configuration Manager to deploy security patches and system updates," writes Radichel. "The case study also describes Target's technical infrastructure, including POS system information."

Compromise third-party vendor

The attackers backed their way into Target's corporate network by compromising a third-party vendor. The number of vendors targeted is unknown. However, it only took one. That happened to be Fazio Mechanical, a refrigeration contractor.

A phishing email tricked at least one Fazio employee, allowing Citadel, a variant of the Zeus banking trojan, to be installed on Fazio computers. With Citadel in place, the attackers waited until the malware offered what they were looking for -- Fazio Mechanical's login credentials.
At the time of the breach, all major versions of enterprise anti-malware detected the Citadel malware. However, unsubstantiated sources mentioned Fazio used the free version of Malware bytes anti-malware, which offered no real-time protection being an on-demand scanner.

Leveraging Target's vendor-portal access

Most likely Citadel also gleaned login credentials for the portals used by Fazio Mechanical. With that in hand, the attackers got to work figuring out which portal to subvert and use as a staging point into Target's internal network. Target hasn't officially said which system was the entry point, but Ariba portal was a prime candidate.

Brian Krebs interviewed a former member of Target's security team regarding the Ariba portal, "Most, if not all, internal applications at Target used Active Directory (AD) credentials and I'm sure the Ariba

system was no exception," the administrator told Krebs. "I wouldn't say the vendor had AD credentials, but internal administrators would use their AD logins to access the system from inside. This would mean the server had access to the rest of the corporate network in some form or another." According to Bloomberg Business, a malware detection tool made by the computer security firm FireEye was in place and sent an alarm, but the warning went unheeded.

Next Stop, Target's Point of Sale (POS) Systems

In an iSIGHT Partners report, details reveal about a malware Trojan. PoS Ram was used to infect Target's POS system. The "RAM-scraping" portion of the POS malware grabs credit or debit card information from the memory of POS-devices as cards are swiped. This technique allowed attackers to steal data from POS terminals that lacked internet access.

Once the credit/debit card information was secure on the dump server, the POS malware sent a special ICMP (ping) packet to a remote server. The packet indicated that data resided on the dump server. The attackers then moved the stolen data to off-site FTP servers and sold their booty on the digital black market.

CHAPTER 5: GENERAL SUMMARY OF SECURITY TIPS

General Summary of Security Tips

- **USBs** – In general, do not let people who do not work at your company plug usbs, keyboards, or any other devices into your computer. This method is commonly used by hackers to gain access to private data on the pc. USB ports can be disabled to physically secure a computer.

Figure 5.1: USB Safety Tips

- **Reporting Possible Breaches** – Any breaches must be brought to the attention of a supervisor immediately so that proper actions can be taken to prevent further damages or even irreversible changes.
- **Firewalls and Antivirus** – Always keep your firewall and Antivirus programs turned on and up to date. These are essential basics as they are the last barrier between data security and data breach.
- **Turning off or signing off equipment/computer** – Always sign out of your computer when you leave your desk so you don't leave active connections and risk chances for creating the perfect bridge for a cybersecurity breach. Although this may be annoying, this is a very important thing to do because anyone using your login credentials could be seen as acting on your behalf, which may be detrimental to your reputation, role, and ultimately cause damages to your company database, information, network, and equipment, and could potentially affect thousands of customers connected to your network as well.
- **Installing** – Always seek the approval of the IT Department when it comes to installing a piece of software on your computer. In general, do not download programs if you have even a slight doubt that they are malicious. There are hundreds of programs out there that were created by malicious hackers.
- **Updating** – Always update all the programs on your computer when it comes time to

update them. There have been many cases where hackers have used certain vulnerabilities in programs to gain access to your computer. These are usually solved in the updates for these programs.

- **Basic Network Security** – If at all possible, try to be on site when it comes to accessing your company network. This will reduce a lot of problems that may arise.

- **Outside Company Access of Sensitive Data** - Accessing company network from the outside should be the last resort. Generally, try to avoid public networks. Always make sure there is a HTTPS, with a green lock to the left of the URL address bar of your web browser. Again, the best thing to do is to avoid accessing the internal network of your company from offsite. This will solve a lot of issues. If you have to access the internal server, have the IT department set up a VPN. This will protect your company from some of the dangers of accessing the network from offsite.

- **Social Engineering** – Social engineering is essentially a "low tech" way for hackers to gain access to a computer. They can use any number of techniques to make you give up information you weren't supposed to. Be ready and be aware of these phishing tactics and report suspicious activity.

- **Think Before you Click** – When in doubt of an email call to verify the sender and message before clicking.

- **Never Become Complacent** – When companies put in policies and are satisfied with them but do not spend the effort to keep them updated constantly, this lends way to them being outdated, causing vulnerabilities. Furthermore, some companies have added wireless devices to their inventory without updating their policies about how end users should use them. What is the use of having technologically advanced devices if the employees don't know how to use them or understand how to troubleshoot the problem if they have no clue what or how the device works. So, keep all personnel informed of new changes and keep unified communication throughout your entire company.

- **Invest in Security Awareness** – Whether or not a company is taking security awareness for their end users seriously is pretty clear simply by looking at their budgets. Have they set aside money to make sure their employees are aware of the risks and how to defend against them? Too many companies spend the bulk of their IT security budgets on security software. Those platforms do no good, though, when the user can be manipulated into allowing the attacker access.

- **Regular Testing Must Be Done** – Testing must be a priority with "live fire" drills. This is the only way to make sure your efforts are truly producing results. The only alternative is finding out you've been compromised. Conduct drills in which someone will try to phish their employees simply to see if they'd fall for it. The test can be analyzed and trends formed so that you can examine the results and cross train your personnel appropriately.

- **Keep Everyone Updated About the State of Cyber Security** – Whoever is in charge of creating your end user security policy must understand the evolving landscape of threats. The Cyber Security Team cannot do a good job of protecting the company if they don't know what is out there. As far as your end users go, regular reminders are an excellent way to make sure they continue to keep security a priority. They should be reminded of new forms of attacks. They should understand the fallout that occurs after a cybercriminal is successful. Telling them only about the big companies getting hacked is good too. However, ideally, show them examples that will resonate because they happened in your industry or to companies similar in size.

- **Make it Easy to Receive Feedback** – Once you begin instituting a serious push for security awareness amongst end users, you have to expect false alarms. People with the best intentions will report phishing attempts that are actually from benign sources. This should be encouraged and never reprimanded. It is better to be safe than sorry. You want people erring on the side of being overly cautious, so make sure no one is allowed to feel embarrassed for coming forward when they were mistaken.

- **Alternatively, you can give employees a chance to report potential vulnerabilities anonymously**. A staff member may know that one of their coworkers isn't properly securing their device when on the road, but they don't want to deal with the consequences of reporting them. If you approach this situation with anonymous reporting, you'll be able to address the problem, learn from it, and prevent it from ever happening again without unnecessarily bringing pressure on people being in the limelight.

- **Don't wait to begin addressing securing awareness amongst your end users.** Putting off the necessary security protection measures and stalling it just another day, could be a chance for your organization to be compromised at any moment in time. Begin with updating and creating a policy and then implementing it across your staff.