An overview of Cyber Security on several remote areas- A case study based upon the preliminary stage

Syed Jamaluddin Ahmad, Dr. Jebunnahar, Roksana Khandoker, Farzana Nawrin

Abstract— **The problems that confront today's leaders are substantial and diverse: how to protect a nation's most critical infrastructure from cyber attack; how to organize, train, and equip a military force to prevail in the event of future conflict in cyberspace; how to deter nation-state and terrorist adversaries from conducting attacks in cyberspace; how to control escalation in the event of a conflict in cyberspace; and how to leverage legal and policy instruments to reduce the national attack surface without stifling innovation. These are just a sample of the motivating questions that drive our work.**

Index Terms—**Cyber Security, cyber attack, cyber space.**

I. Phenomenon of Cyber Security

Cyber security refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access.

According to Forbes, the global cyber security market is expected to reach 170 billion by 2020. This rapid market growth is being fueled by an array of technology trends, including the onslaught of initiatives with ever-evolving security requirements, like "bring your own device" (BYOD) and the internet of things (IoT); the rapid adoption of cloud-based applications and workloads, extending security needs beyond the traditional data center; and stringent data protection mandates, such as the European Union's General Data Protection Regulation and the National Institute of Security Technology (NIST) Cyber security Framework.

II. Why Cyber Security is Required

The core functionality of cyber security involves protecting information and systems from major cyber threats. These cyber threats take many forms (e.g., application attacks, malware, ransom ware, phishing, exploit kits). Unfortunately, cyber adversaries have learned to launch automated and sophisticated attacks using these tactics – at lower and lower costs. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most disruptive form, cyber threats often take aim at secret, political, military or infrastructural assets of a nation, or its people. Some of the common threats are outlined below in more detail.

- Cyber terrorism is the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunication infrastructures.
- Cyber warfare involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. In the U.S. and many other nations, cyber warfare has been acknowledged as the fifth domain of warfare (following land, sea, air and space). Cyber warfare attacks are primarily executed by hackers who are well-trained in exploiting the intricacies of computer networks, and operate under the auspices and support of nation-states. Rather than "shutting down" a target's key networks, a cyber warfare attack may intrude into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.
- Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyber espionage is most often used to gain strategic, economic, political or military advantage, and is conducted using cracking techniques and malware.

III. How to Maintain Effective Cyber security

Historically, organizations and governments have taken a reactive, "point product" approach to combating cyber threats, cobbling together individual security technologies – one on top of another – to protect their networks and the valuable data within them. Not only is this method expensive and complex, but news of devastating cyber breaches continues to dominate headlines, rendering this method ineffective. In fact, given the pervasiveness of data breaches, the topic of cyber security has catapulted to the top of the priority list for boards of directors, which are seeking a far less risky way.

Instead, organizations can consider a natively integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, prevention-based protection – on the endpoint, in the data center, on the network, in public and private clouds, and

Syed Jamaluddin Ahmad, Assistant Professor, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh,
Mobile No.: +8801633628612

Dr. Jebunnahar, Associate Professor, Department of Computer Science & Engineering, , Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh, Mobile No.: +8801761853080

Roksana Khandoker, Senior Lecturer, Department of Computer Science & Engineering, University of South Asia, City: Dhaka, Country: Bangladesh, Mobile No.: +8801737157856

Farzana Nawrin, Lecturer, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh, Mobile No.: +8801686521152

across SaaS environments. By focusing on prevention, organizations can prevent cyber threats from impacting the network in the first place, and reduce overall cyber security risk to a manageable degree.

IV. The Importance of Cyber Security

A. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describe the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

V. CHALLENGES OF CYBER SECURITY

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- **Network security**
- **Application security**
- **Endpoint security**
- **Data security**
- **Identity management**
- **Database and infrastructure security**
- **Cloud security**
- **Mobile security**
- **Disaster recovery/business continuity planning**
- **End-user education**

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

VI. MANAGING CYBER SECURITY

The National Cyber Security Alliance, through SafeOnline.org, recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security management across all business practices. NCSA advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected." NCSA's guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization's "crown jewels," or your most valuable information requiring protection; identifying the threats and risks facing that information; and outlining the damage your organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way your company collects, stores, and secures data, such as PCI-DSS, HIPAA, SOX, FISMA, and others. Following a cyber risk assessment, develop and implement a plan to mitigate cyber risk, protect the "crown jewels" outlined in your assessment, and effectively detect and respond to security incidents. This plan should encompass both the processes and technologies required to build a mature cyber security program. An ever-evolving field, cyber security best practices must evolve to accommodate the increasingly sophisticated attacks carried out by attackers. Combining sound cyber security measures with an educated and security-minded employee base provides the best defense against cyber criminals attempting to gain access to your company's sensitive data. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures.

VII. Critical Infrastructure

Critical infrastructure includes the cyber-physical systems that society relies on, including the electricity grid, water purification, traffic lights and hospitals. Plugging a power plant into the internet, for example, makes it vulnerable to cyber attacks. The solution for organizations responsible for critical infrastructure is to perform due diligence to protect understand the vulnerabilities and protect against them. Everyone else should evaluate how an attack on critical infrastructure they depend on might affect them and then develop a contingency plan.

VIII. Network Security

Network security guards against unauthorized intrusion as well as malicious insiders. Ensuring network security often requires trade-offs. For example, access controls such as extra logins might be necessary, but slow down productivity.

Tools used to monitor network security generate a lot of data — so much that valid alerts are often missed. To help better manage network security monitoring, security teams are increasingly using machine learning to flag abnormal traffic and alert to threats in real time.

IX. Cloud Security

The enterprise's move into the cloud creates new security challenges. For example, 2017 has seen almost weekly data breaches from poorly configured cloud instances. Cloud providers are creating new security tools to help enterprise users better secure their data, but the bottom line remains: Moving to the cloud is not a panacea for performing due diligence when it comes to cyber security.

X. Application Security

Application security (AppSec), especially web application security, has become the weakest technical point of attack, but few organizations adequately mitigate all the OWASP Top Ten web vulnerabilities. AppSec begins with secure coding practices, and should be augmented by fuzzing and penetration testing.
Rapid application development and deployment to the cloud has seen the advent of DevOps as a new discipline. DevOps teams typically prioritize business needs over security, a focus that will likely change given the proliferation of threats.

Internet of things (IoT) security
IoT refers to a wide variety of critical and non-critical cyber physical systems, like appliances, sensors, printers and security cameras. IoT devices frequently ship in an insecure state and offer little to no security patching, posing threats to not only their users, but also to others on the internet, as these devices often find themselves part of a botnet. This poses unique security challenges for both home users and society.

XI. Types of Cyber Threats

Common cyber threats fall under three general categories:
Attacks on confidentiality: Stealing, or rather copying, a target's personal information is how many cyber attacks begin, including garden-variety criminal attacks like credit card fraud, identity theft, or stealing bitcoin wallets. Nation-state spies make confidentiality attacks a major portion of their work, seeking to acquire confidential information for political, military, or economic gain.
Attacks on integrity: Also known by its common name, sabotage, integrity attacks seek to corrupt, damage, or destroy information or systems, and the people who rely on them. Integrity attacks can be subtle — a typo here, a bit fiddled there — or a slash and burn campaign of sabotage against a target. Perpetrators can range from script kiddies to nation-state attackers.
Attacks on availability: Preventing a target from accessing their data is most frequently seen today in the form of ransomware and denial-of-service attacks. Ransomware encrypts a target's data and demands a ransom to decrypt it. A denial-of-service attack, typically in the form of a distributed denial-of-service (DDoS) attack, floods a network resource with requests, making it unavailable.
The following describes the means by which these attacks are carried out.

XII. Social Engineering

Attackers aren't going to hack a computer if they can hack a human instead. Socially engineered malware, often used to deliver ransomware, is the No. 1 method of attack (not a buffer overflow, misconfiguration, or advanced exploit). An end-user is tricked into running a Trojan horse program, often from a website they trust and visit often. Ongoing user education is the best countermeasure against this attack.

XIII. Phishing Attacks

Sometimes the best way to steal someone's password is to trick them into revealing it This accounts for the spectacular success of phishing. Even smart users, well-trained in security, can fall for a phishing attack. That's why the best defense is two-factor authentication (2FA) — a stolen password is worthless to an attacker without a second factor, such as hardware security token, or soft token authenticator app on the user's phone.

XIV. Unpatched Software

It's hard to blame your enterprise if an attacker deploys a zero-day exploit against you, but failure to patch looks a lot like failure to perform due diligence. If months and years pass after disclosure of a vulnerability, and your enterprise has not applied that security patch, you open yourself to accusations of negligence. Patch, patch, patch.
Social media threats
Catfishing isn't just for the dating scene. Believable sock puppet accounts can worm their way through your LinkedIn network. If someone who knows 100 of your professional contacts strikes up a conversation about your work, are you going to think it strange? Loose lips sink ships. Expect social media espionage, of both the industrial and nation-state variety.

XV. Advanced Persistent Threats

Speaking of nation-state adversaries, your enterprise has them. Don't be surprised if multiple APTs are playing hide-and-go-seek on your corporate network. If you're doing anything remotely interesting to someone, anywhere, you need to consider your security posture against sophisticated APTs. Nowhere is this more true than in the technology space, an industry rich with valuable intellectual property many criminals and nations will not scruple to steal.

XVI. Cybersecurity Careers

Executing a strong cyber security strategy requires you have the right people in place. The demand for professional cyber security folk has never been higher, from the C-suite down to the security engineers working on the front lines. Security leaders have elbowed their way into the C-suite and boardrooms, as protecting company data becomes mission critical for organizations. A chief security officer (CSO) or chief information security officer (CISO) is now a core management position that any serious organization must have.
Roles have also grown more specialized. The days of the generalist security analyst are fading fast. Today a penetration tester might focus on application security, or network security, or phishing users to test security awareness. Incident response may see you on call 24/7. The following roles are the foundation of any security team.

XVII. CISO/CSO

The CISO is a C-level management executive who oversees the operations of an organization’s IT security department and related staff. The CISO directs and manages strategy, operations, and the budget to protect an organization’s information assets.
Security analyst
Also referred to as cyber security analyst, data security analyst, information systems security analyst, or IT security analyst, this role typically has these responsibilities:

- Plan, implement and upgrade security measures and controls
- Protect digital files and information systems against unauthorized access, modification or destruction
- Maintain data and monitor security access

- Conduct internal and external security audits
- Manage network, intrusion detection and prevention systems
- Analyze security breaches to determine their root cause
- Define, implement and maintain corporate security policies
- Coordinate security plans with outside vendors

XVIII. SECURITY ARCHITECT

A good information security architect straddles the business and technical worlds. While the role can vary in the details by industry, is that of a senior-level employee responsible to plan, analyze, design, configure, test, implement, maintain, and support an organization's computer and network security infrastructure. This requires knowing the business with a comprehensive awareness of its technology and information needs.

XIX. SECURITY ENGINEER

The security engineer is on the front line of protecting a company's assets from threats. The job requires strong technical, organizational and communication skills. IT security engineer is a relatively new job title. Its focus is on quality control within the IT infrastructure. This includes designing, building, and defending scalable, secure, and robust systems; working on operational data center systems and networks; helping the organization understand advanced cyber threats; and helping to create strategies to protect those networks.

A. The 5 types of cyber attack you're most likely to face

1) Don't be distracted by the exploit of the week. Invest your time and money defending against the threats you're apt to confront

As a consultant, one of the biggest security problems I see is perception: The threats companies think they face are often vastly different than the threats that pose the greatest risk. For example, they hire me to deploy state-of-the-art public key infrastructure (PKI) or an enterprise-wide intrusion detection system when really what they need is better patching.

The fact is most companies face the same threats -- and should be doing their utmost to counteract those risks. Here are the five most common (and successful) types of cyber attack.

B. Socially engineered malware

Socially engineered malware, lately often led by data-encrypting ransomware, provides the No. 1 method of attack (not a buffer overflow, misconfiguration or advanced exploit). An end-user is somehow tricked into running a Trojan horse program, often from a website they trust and visit often. The otherwise innocent website is temporarily compromised to deliver malware instead of the normal

XX. WEBSITE CODING.

The maligned website tells the user to install some new piece of software in order to access the website, run fake antivirus software, or run some other "critical" piece of software that is unnecessary and malicious. The user is often instructed to click past any security warnings emanating from their browser or operating system and to disable any pesky defenses that might get in the way.

Sometimes the Trojan program pretends to do something legitimate and other times it fades away into the background to start doing its rogue actions. Socially engineered malware programs are responsible for hundreds of millions of successful hacks each year. Against those numbers, all other hacking types are just noise.

Countermeasure: Social engineered malware programs are best handled through ongoing end-user education that covers today's threats (such as trusted websites prompting users to run surprise software). Enterprises can further protect themselves by not allowing users to surf the web or answer email using elevated credentials. An up-to-date anti-malware program is a necessary evil, but strong end-user education provides better bang for the buck.

XXI. PASSWORD PHISHING ATTACKS

Coming a close second are password phishing attacks. Approximately 60 to 70 percent of email is spam, and much of that is phishing attacks looking to trick users out of their logon credentials. Fortunately, anti-spam vendors and services have made great strides, so most of us have reasonably clean inboxes. Nonetheless, I get several spam emails each day, and a least a few of them each week are darned good phishing replicas of legitimate emails.

I think of an effective phishing email as a corrupted work of art: Everything looks great; it even warns the reader not to fall for fraudulent emails. The only thing that gives it away is the rogue link asking for confidential information.

XXII. COUNTERMEASURE:

The primary countermeasure to password phishing attacks is to have logons that can't be given away. This means two-factor authentication (2FA), smartcards, biometrics and other out-of-the-band (e.g., phone call or SMS message) authentication methods. If you can enable something other than simple logon name/password combinations for your logons, and require only the stronger methods, then you've beat the password-phishing game.

If you're stuck with simple logon name/password combinations for one or more systems, make sure you use accurate-as-can-be anti-phishing products or services, and decrease the risk through better end-user education. I also love browsers that highlight the true domain name of a host in a URL string. That way windowsupdate.microsoft.com.malware.com, for example, is more obvious.

XXIII. UNPATCHED SOFTWARE

Coming in close behind socially engineered malware and phishing is software with (available but) unpatched vulnerabilities. The most common unpatched and exploited programs are browser add-in programs like Adobe Reader and other programs people often use to make surfing the web easier. It's been this way for many years now, but strangely, not a single company I've ever audited has ever had perfectly patched software. It's usually not even close. I just don't get it.

Countermeasure: Stop what you're doing right now and make sure your patching is perfect. If you can't, make sure it's perfect around the most exploited products, whatever they happen to be in a given time period. Everyone knows that better patching is a great way to decrease risk. Become one of the few organizations that actually does it. Better yet, make sure that you're 100 percent patched on the programs most likely to be exploited versus trying unsuccessfully to be fully patched on all software programs.

A. Social media threats

Our online world is a social world led by Facebook, Twitter, LinkedIn or their country-popular counterparts. Social media threats usually arrive as a rogue friend or application install request. If you're unlucky enough to accept the request, you're often giving up way more access to your social media account than you bargained for. Corporate hackers love exploiting corporate social media accounts for the embarrassment factor to glean passwords that might be shared between the social media site and the corporate network. Many of today's worst hacks started out as simple social media hacking. Don't underestimate the potential.

Countermeasure: End-user education about social media threats is a must. Also make sure that your users know not to share their corporate passwords with any other foreign website. Here's where using more sophisticated 2FA logons can also help. Lastly, make sure all social media users know how to report a hijacked social media account, on their own behalf, or someone else's. Sometimes it is their friends who notice something is amiss first.

B. *Advanced persistent threats*

I know of only one major corporation that has not suffered a major compromise due to an advanced persistent threat (APT) stealing intellectual property. APTs usually gain a foothold using socially engineered Trojans or phishing attacks.

A very popular method is for APT attackers to send a specifi phishing campaign -- known as spearphishing -- to multipl employee email addresses. The phishing email contains a Troja attachment, which at least one employee is tricked into running After the initial execution and first computer takeover, AP attackers can compromise an entire enterprise in a matter c hours. It's easy to accomplish, but a royal pain to clean up.

XXIV. Countermeasure:

Detecting and preventing an APT can be difficult, especially i the face of a determined adversary. All the previous advic applies, but you must also learn to understand the legitimat network traffic patterns in your network and alert on unexpecte flows. An APT doesn't understand which computers normall talk to which other computers, but you do. Take the time now t start tracking your network flows and get a good handle of what traffic should going from where to where. An APT will mess up and attempt to copy large amounts of data from a server to some other computer where that server does not normally communicate. When they do, you can catch them.

Other popular attack types such as SQL injection, cross-site scripting, pass-the-hash and password guessing aren't seen nearly at the same high levels as the five listed here. Protect yourself against the top five threats and you'll go a long way to decreasing risk in your environment.

More than anything, I strongly encourage every enterprise to make sure its defenses and mitigations are aligned with the top threats. Don't be one of those companies that spends money on high-dollar, high-visibility projects while the bad guys continue to sneak in using routes that could have easily been blocked.

Lastly, avail yourself of a product or service that specializes in detecting APT-style attacks. These products or services either run on all your computers, like a host-based intrusion detection service, or collate your event logs looking for signs of maliciousness. Long gone are the days where you'll have a hard time detecting APT. Myriad vendors have now filled the earlier void and are waiting to sell you protection.

Overall, figure out what your enterprise's most like threats will be and prepare for those the most. Too many companies waste resources concentrating on the wrong, less likely scenarios. Use their threat intelligence as compared to your environment's make up and vulnerabilities, and determine what you should be preparing for the most.

XXV. The Cost of Cyber Attacks

Now, back to Kaspersky Lab's news about the average cost of a data breach. Globally, the cost of a data breach for enterprises has risen 11 percent in 2017. In the U.S., the average cost of a cyber attack for enterprises grew from $1.2 million in 2016 to $1.3 million in 2017. That's 10 times higher than the $117K cost of a breach for SMBs.

Overall, businesses are looking at IT security as more of an investment in 2017. In fact, IT security budgets are up, reaching 18 percent for enterprises compared to 16 percent in 2016. Even small businesses with fewer resources are investing more in IT security budgets this year — 14 percent compared to 13 percent in 2016.

In North America, the Kaspersky Lab study found that the following incidents have the most severe financial impact in 2017:

Financial impact on enterprises

1. Physical loss of devices or media containing data ($2.8 million)
2. Incidents affecting IT infrastructure hosted by a third party ($2.2 million)
3. Electronic leakage of data ($1.9 million)
4. Inappropriate IT resource use by employees ($1.1 million)
5. Viruses and malware ($519,000)

Financial impact on SMBs

1. Targeted attacks ($188,000)
2. Incidents involving non-computing connected devices ($152,000)
3. Physical loss of devices or media containing data ($83,000)
4. Inappropriate IT resource use by employees ($79,000)
5. Viruses and malware ($68,000)

The top "pain points" with the largest average costs after a breach for enterprises include $207,000 for internal staff wages, $172,000 for improved software/infrastructure, and $153,000 spent on cybersecurity training.

The top pain points for SMBs in 2017 include $21,000 in lost business and another $21,000 in costs related to employing external professionals.

When a third party is breached, that security failure is one of the most damaging to enterprises.

The Internet of Things (IoT) can be another extremely damaging security failure, given the widespread use of factory default passwords that allow IoT devices to become hosts for botnets.

XXVI. Highest IT Security Budgets

Organizations involved in government, including defense, and financial institutions reported having the highest IT security budgets — over $5 million. IT and telecom companies, as well as utilities and power companies, spend about $3 million on IT security budgets.

However, as Kaspersky Lab noted, when it comes what is spent on IT security "per head," government organizations spend $959 per head, while IT and telecoms spend $1,258 per head, utilities companies spend $1,344 per head, and financial firms spend $1,436 per head.

XXVII. Lowest IT security budgets

Industrial firms, which rely on industrial control systems (ICS) infrastructure, have some of the lowest IT security budgets at $748,000 even though attacks on ICS infrastructure are up 5 percent in 2017.

How companies spend their IT security budgets

After businesses increase IT security budgets, 39 percent goes toward protecting increasingly complex IT infrastructure. Improving the level of specialist security experts is another important expenditure, up to 32 percent in 2017 compared to 29 percent in 2016.

The cost of consultant advice is also up, with businesses using 11 percent of their security budgets in 2017, up 1 percent from last year. There was a significant drop in increasing security budgets for new business activities or expansions, with spending dropping from 45 percent in 2016 to 28 percent in 2017.

For more information, you can download a copy of Kaspersky's report, IT Security: Cost Center or Strategic Investment? (Registration required.) You can also tap into IT security strategies by checking out a new tool, Kaspersky IT Security Calculator.

Advanced Detection and Prevention

Today's attacks are designed to bypass your organization's defenses, regardless of your industry or size. In fact, while 68% of observed malware appears only at one organization, 80% of observed malware appears once, period. Signature-based defenses cannot protect against single-use malware. Even more importantly, in many cases, attackers eschew malware for social engineering and other tactics.

Failure of standard detection methods

Conventional detection methods fail because they are incomplete:

- Indicators are ephemeral. They can only be used to provide information about a specific, retrospective point in time data point. They are a piece of the puzzle, but cannot tell the entire story. You need more evidence to build the context necessary to anticipate future attacks.
- Integrated perimeter controls, which include firewalls and sandboxes, often execute traffic objects sequentially, one at a time, in siloed environments and completely miss attacks that use multiple steps or non-digital steps.
- Security analytics can identify anomalies and activities that have previously been unseen. However, what informs these algorithms? Absent of knowledge of the attacker's behavior, attacks can easily evade these defensive measures.
- Threat intelligence provides insights into the attacker's tactics and techniques and may even correlate ongoing activity to an attacker. However, security programs can't operationalize that knowledge into your detection architecture.

FireEye detection takes a different approach

A well-designed security architecture must detect even the most sophisticated attacks while ignoring the distractions of false alerts. Proven FireEye detection blends detection analytics and machine learning, with threat intelligence into the patented MVX engine to:

- Intuitively understand and codify the tools, techniques and procedures (TTPs) of attackers; evidence is broken down to an atomic level, and translated into products. Fusing detection research and analytics with visibility into the threat landscape delivers the insights to identify never before seen techniques and tools. Organizations are no longer trying to manually perform weak signal analysis to find the attack buried in the noise.
- Use continually tuned and codified intelligence to reverse engineer attacker TTPs, track malware to its source, and perform other advanced detection functions

The automated detection engine is updated at least every 60 minutes with knowledge engineering of insights captured from incident responders from the world's most sophisticated attacks, deep research gleaned from inside attacker systems, and millions of sensors monitoring for evidence of even the most sophisticated attacks worldwide. Fusing these detection techniques and sources of insights gives you the ability to identify never-before-seen attack tactics and tools.

Cyber Security ROI for CEOs

Avoid the cost of cyber crime with the benefits of security

Every responsible CEO relies on cyber security to safeguard their company's systems, and their customers' and partners' data. With the right investments in cyber security, you can protect your organization's data, preserve your customers' trust, and manage your costs and security resources wisely.

The Myths of Cyber Security as Usual

Myth 1: More cyber security is better cyber security.

The reality: More traditional cyber security, such as antivirus software and firewalls, is a poor choice for a CEO. Increasing standard cyber security usually costs more time, money and personnel. If security teams don't get training and build expertise with new security tools, they can often misinterpret alerts from those tools, ending up with an increase in false positives. This takes time away from real threats and results in poorer overall security.

Myth 2: Better technology provides better security.

The reality: This holds true only up to a point. Cyber attacks are masterminded by people. People will always find ways around static technology. CEOs should install an Adaptive Defense approach that includes technology, intelligence and expertise to successfully combat modern cyber threats.

Myth 3: Detection and prevention are the primary measures of success for security.

The reality: CEOs need to shift the security mindset to include the entire threat life cycle. Better measures of success include:

- Number of incidents resolved
- Speed of incident resolution
- Potential business impact of the incident

Sound measures of success, strong technology, timely intelligence and knowledgeable experts are the cornerstones of security investments that will pay off for your company in both the short and long term.

Working with FireEye can deliver an almost 10-fold return on your cyber security investment by preventing more attacks, responding effectively to breaches and easing the transition to a modern, nimble and more cost-efficient approach to dealing with real security issues.

Best Defense Against Spear Phishing

Recognize and defend against the signs of an advanced cyber attack

Spear phishing is a very simple, yet targeted and dangerous email-based cyber attack.You've probably seen a spear-phishing email before:

- Could you please log into your file sharing account and review the following proposal?
- We noticed an issue with your social media account. Follow the attached instructions to fix the issues as soon as possible.
- There's been unauthorized activity on your bank account. Click here to log in and fix the problem.

Spear phishing: the who and the why

Anyone can be the target of a spear-phishing attack, whether they accidentally click on an unsolicited survey response or get bamboozled by a fake alert from their bank. While an attacker may not be interested in you specifically, you can be their foothold into a secure computer system that may contain the PII of customers, executives and other personnel as well as critical data, such as intellectual property and financials. In that sense, we are all critical to the safety of our own PII and the business systems we are part of. If you're in finance, you have access to critical company data. If you're in sales, you have access to lists of customers and prospects. If you're in facilities, you may have access to onsite service-call schedules. Everyone has value.

Spear-phishing attacks are not trivial or conducted by random hackers. They are targeted at a specific person, often times by a specific group. Many publicly documented advanced persistent threat (APT) attack groups, including Operation Aurora and the recently publicized FIN4 group, used spear-phishing attacks to achieve their goals.

How to stop spear-phishing attacks

To stop spear-phishing attacks security teams must first train users to recognize, avoid and report suspicious emails—it is important for every employee to recognize that their roles grant them access to different data, the currency of the information economy. Second, security teams must implement, maintain and update security technology and processes to prevent, detect and respond to ever-evolving spear-phishing threats. Finally, security teams must strive to stay ahead of attackers by investing in actively updated threat intelligence and expertise to meet their needs.

One thing is clear: You cannot discover a new spear-phishing attack by looking at it in isolation. This is how conventional point products such as antivirus and anti-spam software operate. While they can detect some known threats, they will fail to detect unknown threats and spear-phishing attacks.

Working with FireEye, you can develop fully integrated security solutions that cover multiple threat vectors. A spear-phishing attempt is often part of a blended attack that uses a combination of email, internet browsing and file shares. FireEye can help connect the dots to discover it in real time. Using a combination of industry-leading technology, threat intelligence and security expertise, FireEye can help identify:

- Which attack groups are likely to use spear phishing
- How attackers choose and approach their targets
- What their ultimate goals are
- What specific steps you can take to prevent or block malicious attacks resulting from spear-phishing emails

To stop spear-phishing attacks and protect your organization's assets with an integrated security posture, see the FireEye Email Security products.

Quantity does not equal quality

When you buy a cyber security solution, you expect to get alerts. And with malware signatures, you certainly will. Signature-based technologies, "next-generation" products and sandboxing solutions look for anything—and everything—they've experienced before. The wide net they often cast generates volumes of alerts for low-risk, low-priority attacks and false positives – benign events incorrectly labeled as attacks. Even worse, these conventional technologies will miss the indicators of unknown attacks, with devastating results.

The cost of indiscriminate alerts

Security teams get up to a thousand if not hundreds of thousands of alerts in a week. Third-party studies tell us that only 19 percent are reliable, and security teams only have time to really investigate four percent of them—and they don't know in advance if that four percent really matter! Consequently, security analysts spend two-thirds of their time investigating false alerts. This wasted effort costs the average company over $1.2 million each year.

To deal with this reality, security teams have a choice:

Pay more now to scale operations, knowing that two-thirds of their money will continue to be wasted on noise

Pay more later when they miss critical alerts and experience a breach that can cost $10,000- $100,000+ per hour in remediation costs

Target Cyber Criminals to Stop Cyber Crime

Focus on the people, then the technology

Cyber criminals, threat actors, hackers—they know cyber crime pays. Your data and technology, stored in networks and the cloud, are vulnerable. And although the tactics, targets and technology of attacks are all important, your most powerful defense against cyber crime is to understand threat actors.

To effectively prevent and respond to cyber crime, you need to establish the motivations and methodology of threat actors. Here are two ways advanced cyber attacks work:

- Targeted – Malware, such as spear phishing, is used to reach a specific machine, individual, network, or organization. This malware tends to be signature-less, or otherwise evades antivirus and other traditional cyber security efforts using the criminal's knowledge of the target.

- Persistent – Advanced cyber attacks are initiated via a series of email, file, web, or network actions. These individual actions might remain undetected by antivirus or other traditional defenses, or be ignored as harmless or low-priority. However, the malware becomes entrenched and pervasive, and culminates in a devastating attack.

Malware that uses both of these methodologies simultaneously presents an advanced persistent threat, or APT. And any organization in any industry can be a target.

XXVIII. What Cyber Criminals Want

You can defend yourself more effectively and efficiently when you learn what cyber criminals want, because you'll understand your high-value vulnerabilities and your significance as a target.

Economic espionage

Economic cyber espionage uses APTs to acquire intellectual property and sensitive information. Ultimately, the threat actor seeks a long-term economic advantage, either for themselves or on behalf of their employer. The primary sponsors of cyber espionage include nation states and businesses competitors. No company is safe, and in fact many network breaches often begin with attacks on secondary targets such as vendors in the primary target's supply chain.

Organized crime

Organized cyber crime uses APTs to realize short-term, rapid financial gain through activities such as credit card theft. Their cyber attacks are designed to evade traditional cyber security measures and remain on a victim’s network for a long period of time. While no business is safe, targets tend to be companies that provide retail and financial services, including banks and credit card processors.

Nuisance threats and hacktivism

Nuisance threats and hacktivist cyber attacks attempt to interfere with daily business operations, defame web properties and make political statements. While embarrassing, they are typically neither targeted nor persistent. While attackers can be individuals, most are groups such as Anonymous and LulzSec who use botnets or spam to target both organizations and individuals.

Anatomy of Advanced Persistent Threats

If you know how they work, you can learn how to stop them

From cyber criminals who seek personal financial information and intellectual property to state-sponsored cyber attacks designed to steal data and compromise infrastructure, today’s advanced persistent threats (APTs) can sidestep cyber security efforts and cause serious damage to your organization. A skilled and determined cyber criminal can use multiple vectors and entry points to navigate around defenses, breach your network in minutes and evade detection for months. APTs present a challenge for organizational cyber security efforts.

Ransomware: the Tool of Choice for Cyber Extortion

Blackmail over the Internet

Ransomware is malware that typically enables cyber extortion for financial gain. Criminals can hide links to ransomware in seemingly normal emails or web pages. Once activated, ransomware prevents users from interacting with their files, applications or systems until a ransom is paid, typically in the form of an anonymous currency such as Bitcoin. Ransomware is a serious and growing cyber threat that often affects individuals and has recently made headlines for broader attacks on businesses. Payment demands vary based on targeted organizations, and can range from hundreds to millions of dollars.

A multitude of ransomware variants exist. In recent years, there has been a significant increase in the brazenness, prominence, frequency and number of ransomware attacks. They include Cryptolocker and its variants such as Kriptovor and Teslacrypt, Cerber, Dridex and Locky and most recently, WannaCry.

Once infected, a victim has little recourse. If they do not pay the ransom, they suffer business down time, loss of sensitive information or any other penalty specified by the attacker. And even when they do pay the ransom, they remain vulnerable to attack from the same attacker or a new one, and reward attackers for their successful tactics.

Usually, if you have to choose whether to pay a cyber ransom, it’s too late.

How to combat ransomware

Ransomware often uses the web or email to reach victim systems, so those are vectors that security teams must monitor for signs of attack.

Web-based attacks tend to use drive-by exploits that target browser, platform or system vulnerabilities, or rely on malicious URLs or malvertising that may redirect users to sites that host exploit kits. Once it takes hold of a system, it can travel to other connected systems or servers on the network. Email-based ransomware is generally used in targeted attacks, and relies on a variety of methods, including phishing, spear sphishing, malicious attachments and URLs.

To properly defend against ransomware, three things need to happen:

The infection process must be thoroughly analyzed to determine the path of attack and system vulnerabilities

The malicious code must be analyzed to determine its purpose and signs of activity (behavior-based analysis)

Access from infected machines to command and control servers (used for data exfiltration or to download additional malware) must be blocked

This defensive approach relies on connecting warning signs across different vectors that are often overlooked by traditional security solutions. Advanced security solutions, such as FireEye Network Security (NX Series), FireEye Email Security (EX Series), or FireEye Email Threat Prevention Cloud (ETP) stop ransomware from taking control by blocking exploit kits, malware downloads and callback communications to the command and control servers. They can also minimize the overall impact of ransomware by tracing its attack path and methodology and sharing threat details to stop future attacks.

REFERENCES

[1]https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

[2] https://digitalguardian.com/blog/what-cyber-security

[3] https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html

[4] https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html

[5] https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html

[6] https://www.mwrinfosecurity.com/our-thinking/targeted-attack-case-studies/

[7] https://www.alertlogic.com/customers/case-studies/

[8] https://www.acorn.gov.au/learn-about-cybercrime

[9] cyber Law

[10] https://www.fireeye.com/current-threats/what-is-cyber-security.html

[11] https://www.fireeye.com/current-threats/detect-and-prevent.html

[12] https://www.fireeye.com/current-threats/what-a-ceo-needs-to-know-about-cyber-security.html

[13] https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html

[14] https://www.fireeye.com/current-threats/tco.html

[15] https://www.fireeye.com/current-threats/stopping-todays-cyber-attacks.html

[16] https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

[17] https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html

[18] combat ransomware

[19] Cyber act 1998

[20] https://www.fireeye.com/solutions/nx-network-security-products.html

[21] Defend your network, data, and users with the fastest, most reliable cyber-attack protection

[22] Remote area [5:6]

[23] Law act. 1992

Syed Jamaluddin Ahmad, achieved Bachelor of Science in Computer Science and Engineering (BCSE) from Dhaka International University, Masters of Science in Computing Science Associates with research: Telecommunication Engineering from Athabasca University, Alberta, Canada and IT-Pro of Diploma from Global Business College, Munich, Germany. Presently Working as an Assistant Professor, Computer Science and Engineering, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was head of the Department of Computer Science & Engineering, University of South Asia from 2012-2014, also Lecturer and Assistant Professor at Dhaka International University from 2005-2007 and 2011-2012 respectively and was a lecturer at Loyalist College, Canada, was Assistant Professor at American International University, Fareast International University, Royal University, Southeast University and Many more. He has **alrea**dy 15th international publications, 12th seminar papers, and conference articles. He is also a founder member of a famous IT institute named Arcadia IT (www.arcadia-it.com). Achieved Chancellor's Gold Crest in 2010 for M.Sc. in Canada and Outstanding result in the year of 2005. and obtained "President Gold Medal" for B.Sc.(Hon's). Best conductor award in Germany for IT relevant works. Membership of "The NewYork International Thesis Justification Institute, USA, British Council Language Club, National Debate Club, Dhaka, English Language Club and DIU . Developed projects: Mail Server, Web Server, Proxy Server, DNS(Primary, Secondary, Sub, Virtual DNS), FTP Server, Samba Server, Virtual Web Server, Web mail Server, DHCP Server, Dial in Server, Simulation on GAMBLING GAME Using C/C++, Inventory System Project, Single Server Queuing System Project, Multi Server Queuing System Project, Random walk Simulation Project, Pure Pursuit Project (Air Scheduling), Cricket Management Project, Daily Life Management Project, Many Little Projects Using Graphics on C/C++, Corporate Network With Firewall Configure OS:LINUX (REDHAT) Library Management Project Using Visual Basic, Cyber View Network System:Tools:Php OS: Windows Xp Back-end: My SQL Server, Online Shopping: Tools: Php, HTML, XML. OS:Windows Xp, Back-end: My SQL and Cyber Security" Activities-'Nirapad Cyber Jogat, Atai hok ajker shapoth'-To increase the awareness about the laws, 2006 (2013 amendment) of Information and Communication and attended Workshop on LINUX Authentication"-Lead by- Prof. Andrew Hall, Dean, Sorbon University, France, Organized By- Athabasca University, CANADA, April, 2009. His areas of interest include Data Mining, Big Data Management, Telecommunications, Network Security, WiFi, Wimax, 3g, 4g network, UNIX, LINUX Network Security,Programming Language(C/C++ or JAVA), Database (Oracle), Algorithm Design, Graphics Design & Image Processing and Algorithm Design.

Dr. Jebunnahar, achieved Bachelor of Science in Computer Science and Engineering and Master of Computer Science and Engineering from Department of Computers, Complexes, Systems and Networks, Vladimir State Technical University. Ph.D. in Information and Technology from Moscow Lomonosov State Academy of Fine Chemical Technology, Russia. She worked as Chairman, CSE department of European University of Bangladesh. Formerly she worked as Assistant and Associate professor in other university and institution. Presently working as an associate professor and IT in-charge at Shanto-Mariam University of Creative Technology . She did ToT from Humber institute in Canada. She attended many national and international workshops. Her interested area cyber security …

Roksana Khandoker, achieved Bachelor of Science in Computer Science and Engineering (BCSE) from United International University, Masters of Science in Computer Science and Engineering from University of South Asia. Presently Working as a Senior Lecturer, Computer Science and Engineering, University of South Asia, Dhaka, Bangladesh. Formerly, was also a lecturer at different poly-technique institutes. She has 4th international journals and attended different international and national conferences. She is the Chairman of the famous IT institute named Arcadia IT and Chairman of Brighton International Alliance. Her areas of interest include Data Mining, Big Data Management, Telecommunications, Network Security, WiFi, Wimax, 3g and 4g network.

Farzana Nawrin achieved Bachelor of Science in Computer Science and Engineering (BCSE) from Dhaka City College under National University, Masters of Science in Computer Science from Jahangirnagar University. She achieved 1st class 1st both B.Sc. and M.Sc. degree. Presently working as a lecturer, Computer Science and Engineering department, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was also a lecturer of Computer Science and Engineering department of Dhaka City College under National University. She has done two thesis about network security in her B.Sc. and M.Sc. level. She has two international journal.She was also attended many national workshop. She has got special training from Bangladesh Institute of Design and Development(BIDD). She has special certification in CCNA and CompTIA A+. Her areas of interest include Network Security, Telecommunication, System analysis, Automata Design, Routing and Switching, Design and Analysis Compiler, Wifi,Wimax,3g and 4g Network.