Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 2, February 2017, pg.107 – 118

EMERGING AND UPCOMING THREATS IN CYBER SECURITY IN 21 CENTURY

Navnita Nandakumar
Stella Maris College, Chennai -600093, Tamil Nadu, INDIA
navnitanandakumar@gmail.com
Mobile: 8754470886

Dr. I. Lakshmi
Stella Maris College, Chennai -600093, Tamil Nadu, INDIA
lakshmi.i@stellamariscollege.org
Mobile: 9677051822

Abstract: ***The exponential growth of the Internet interconnections has led to a significant growth of cyber- attack incidents often with disastrous and grievous consequences. Malware is the primary choice of weapon to carry out malicious intents in the cyberspace, either by exploitation into existing vulnerabilities or utilization of unique characteristics of emerging technologies. The development of more innovative and effective malware defense mechanisms has been regarded as an urgent requirement in the cyber security community. To assist in achieving this goal, we first present an overview of the most exploited vulnerabilities in existing hardware, software, and network layers. This is followed by critiques of existing state-of-the-art mitigation techniques as why they do or don't work. We then discuss new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology, and critical infrastructure. Finally, we describe our speculative observations on future research directions.***

Keywords: Cyber security; Malware; emerging technology trends; emerging cyber threats; Cyber-attacks and countermeasures.

1. Introduction

The collection and analysis of big datasets has shed light on a variety of subjects— from profiling consumers' buying habits to forecasting the loss of Arctic ice. Companies, from Google to Apple to traditional car makers, are focusing great efforts on creating autonomous vehicles with a near-term goal of a driverless car on the road by 2020. These trends continue to grow despite obvious dangers — ever-present devices and online tracking allow us to measure our

activities, but give other third parties unprecedented access to monitor those same habits. Automated systems are increasingly removing humans from operational loops, making everything from driving cars to diagnosing diseases less prone to human error, but at the same time, requiring that each device be trusted— a technology safeguard that does not yet fully exist. Attackers have shown that these dangers are not just theoretical. As many as 32 lakh debit cards Belonging to various Indian banks were compromised in 2016, resulting in the loss of Rs 1.3 crore in fraudulent transactions as per NPCI. The infamous hacker group Legion made headlines in the sub-continent after hacking into the Twitter accounts and partial email dumps of prominent public figures such as politician Rahul Gandhi, businessman Vijay Mallya, and NDTV journalists Barkha Dutt and Ravish Kumar. In order to understand the dangers posed by our increasingly digital world, it is imperative to study the potential problems and define necessary solutions. This paper, therefore, attempts to discuss the emerging threats, their potential impact on our digital society and solutions for a safer and more secure future.

2. 2016 Predictions

While avoiding breach altogether is unrealistic, companies can do their best to prepare for compromise so when it comes, they can react quickly and efficiently. FortiGuard Labs lists five cyber security threat predictions to watch for in 2016:

IoT: Great Friend and Sneakiest Foe: The Internet of Things is expected to grow even more in 2016. The possibilities are exciting. However, in 2016, Jason Sabin of DigiCert cautions that, "Hackers will use IoT devices as springboards into corporate networks." Access points multiply as the number of IoT devices used in the workplace increases. Across the board, security professionals agree that IoT will become central to "land and expand" attacks. Hackers will take advantage of vulnerabilities in every area from smart home devices to wearables, compromising corporate-issued devices or corporate networks.

Jail-breaking the Cloud: Hackers are expected to seek out vulnerabilities to compromise host systems as virtualization technologies expand further. Specifically, mobile applications can potentially turn mobile devices into vectors for remote attacks on cloud-based systems.

"Ghostware" Conceals Indictors of Compromise: Contrary to "Blastware," which destroys itself and host systems *if* detected by antivirus software, "Ghostware" extricates data and deletes all evidence of compromise *before* it can even be detected. Subsequently, companies don't even know where to start when seeking out the extent of data loss.

Headless Worms Target Headless Devices: Autonomous, or "headless," attacks are likely to make their headless device debut in 2016. Malware is expected to disseminate from device to device with the expansion of attack surfaces like those found in the IoT.

Two-Faced Malware: Savvy attackers are expected to design a new two-faced malware that will carry out a benign process at runtime, mask its efforts as safe while under inspection, and then execute its malicious process once clear. Additionally, companies face another challenge if

this malware is flagged as safe by their advanced sandboxing techniques. In this case, two-faced malware will escape future inspection by vendors' threat intelligence systems.

2.1 Smartphones and wearable's make consumers easily trackable and the advanced technology they employ is collecting digital breadcrumbs beyond what most would want or know.

Unfortunately, people have few options to limit their exposure to data breaches and unintended use of their data. Moreover, there is a general lack of understanding about how much digital dust people are leaving around— most consumers do not even know what information companies are collecting on them or how they are using it. Businesses are driven to collect more data on consumers to improve operations, posing a significant risk to privacy. The drive to improve business processes and better identify potential customers or markets have businesses collecting as much data as they can. Large consumer services, such as Netflix and Amazon, regularly collect information to better serve or suggest products to their customers. Others, such as package delivery services and restaurant chains, use data to streamline operations and reduce business costs. Yet a whole host of third-party firms, with no relationship to the consumer, also collect data. Visits to the top 100 websites, for example, are tracked by more than 1,300 firms, from social networks to advertising networks to data brokers that receive digital dossiers about website visitors and trade them to other businesses. In many cases, a company's access to data may seem legitimate, but the very fact that a database exists can often lead to unforeseen and unethical uses of the data. In late 2014, the billion-dollar ride-share startup Uber faced criticism for multiple incidents of tracking people without their permission and for making the tracking functionality— what they referred to as the "God View"—available to workers as well as prospective employees. In June, the Electronic Privacy Information Centre filed a complaint with the Federal Trade Commission, charging that they company misled customers about the degree to which they can control their privacy and their ability to opt out of the service's tracking capabilities, among other accusations. But consumers regularly trade access to their data for convenience. People are spending a greater amount of time online or on a device. The average urban adult spends a little over two and a half hours on a computer or smartphone each day, according to studies conducted by Nielsen in 2015. The digital breadcrumbs and governments to form an increasingly detailed picture of their activities. Mobile devices have accelerated the trend. More companies have access to detailed user data through the installation of apps on smartphones. With smartphones, for the first time in human history, we all carry tracking devices. In April 2015, consumer-monitoring firm Nomi was tried for (and subsequently settled) a privacy case brought by the Federal Trade Commission, the government watchdog that protects consumers. Nomi's technology allows stores to track consumers' movements through their aisles for marketing and loyalty programs, but the company could not provide any meaningful way for consumers to opt out of their monitoring. Reversing the trend will be nearly impossible. For one, protecting against monitoring is an almost impossible task for the average consumer. Too often, a person is faced with a choice of agreeing to the slightly distasteful collection of their data or to being completely unable to sign up for a useful service. In addition, the primary mechanism for

notification and consent— privacy policies— have largely failed. Research conducted by the School of Interactive Computing at Georgia Tech University found that few consumers read online policies and that to do so would take the average internet user over 200 hours per year.
Advanced computing and pattern-matching capabilities mean even careful citizens are tracked. Even if a consumer is careful to minimize the information collected by their mobile devices and use pro-privacy technology online, it has become harder to escape notice in the real world. Increased video and signals monitoring of public spaces, paired with the collection of a variety of identifiers — such as license plates, facial images, and smartphone IDs— means that real-world monitoring will increasingly resembles online tracking.
The debate regarding monitoring policy needs to be public, so that a meaningful debate can focus on the issues, it is a policy discussion and a technical discussion. One needs to know what rights one has, regardless of one's knowledge of how many digital breadcrumbs one is leaving behind.
So what can consumers do to control their data? While consumers have little control of data once they opt-in to a relationship with a company, there are some ways the average citizen can maintain certain privacy protections— using software that blocks tracking cookies and deleting cookies regularly, using anonymising networks to defend against network surveillance, deleting apps once they're no longer in use, opting out of location tracking where possible, avoiding the use of the same password in more than one setting and using back-up systems like external hard drives that are not dependent on cloud-based services.

2.2 The shortfall in skilled security workers put companies in peril.

The infrastructure supporting the digital economy is growing more complex. Companies increasingly run their computing systems on virtual machines, cloud services have become a standard business practice and personal mobile devices increasingly creep into the workplace. Yet, despite the influx of technology, there is a significant lack of trained security experts. "The message that everyone is hearing is 'IT everywhere', and not just in the online world," says Mystique Ahamad, professor at the GTRI College of Computing. "The problem is that 'IT everywhere' also requires the need to safeguard IT everywhere, and for that, we need the people." Traditional four-year degrees at colleges and universities will not solve the problem. An estimated 18,000 students graduated with a degree in computer science in 2015, yet when compared to the explosion of software ecosystems, those graduates are not enough, especially since most graduates do not have extensive class time in cyber security topics. "Companies are looking for talent and they want that talent to be security aware," says Bo Rotoloni, co-director of the Institute for Information Security and Privacy (IISP). Five years ago, Intel Corp. began discussing ways to better train college graduates who would be more capable of building secure code. When Intel hires a new computer science or engineering graduate for a security position, it takes about one year to train— or "retool"— them for their work, according to Scoot Buck, University Program Manager for Intel. The company is working to develop educational programs and modules that infuse basic cyber security concepts into courses taken by all computer science students. The parade of major breaches over the past few years has gained the attention of corporate boards. The damage to executive careers has made companies more

willing to provide budget to secure the systems and data. Corporate boards are more focused on security. Yet, businesses have significant room for improvement. The industrial and energy/utilities sectors lag other industries in some aspects of cyber security governance. Security needs to be adopted from the executive offices all the way down to workers' cubicles. If employees are alerted of security as a problem, decisions about strategy and approach would improve, and the whole organization will drive towards a more secure posture. While many companies are focused on the security threat posed by disgruntled workers, almost all companies need to be worried about the threat posed by well-intentioned workers who do not understand security. When most people think of an insider threat, they think of Snowden, the former National Security Agency contractor who copied and leaked classified information without prior authorization, but there is also the unintentional insider threat— who ill-advisedly open a phishing site , or sign up for a website using their work e-mail. Companies need to focus on educating their employees about security issues— teaching them about the dangers of phishing, unencrypted data and lax reactions. Training employees can turn a worker into a security asset, capable of helping detect threats. With education and training requiring years, and possible decades, to address the current shortfall of skilled security specialists, technology and businesses must fill the gaps in the short term. While educating the future generation of security professionals is necessary, it is a long-term solution. In the short term, using cloud and security services to deliver security expertise to a broad base of companies may be the only way forward.
More intelligent security systems that improve the recognition of important security alerts can help businesses better secure their networks and data. A decade ago, companies were just starting to mine their systems' log files for security information and required a team to maintain the capability. Today, such tools consume much more data from a greater variety of IT devices and do much of the initial work to eliminate false alerts. Automation is the key, reducing the workload by better analysis using more data to reduce false pot ivies, this helps find more sophisticated threats. Automation is not just about improving software. Businesses that bring the benefits of automation into security services can help create a foundation of security for client companies. Security-as-a service can allow a single expert to maintain and administer multiple clients, reducing the demand for security experts. Through automation, advanced analytics and a highly trained workforce, security-as-a-service provider Dell Secure Works filters through more than a hundred-and-fifty billion events a day for its four-thousand-two-hundred clients, and whittles them down to about ten billion security events. Those events are then correlated, analyzed, and reduced to less than five thousand potential attacks that require a response, according to the firm. Through that sort of specialized automation, tools and analytics, a singly security worker at a security-as-a-service provider can be far more productive than a lone worker at even a security savvy firm, according to Jon Ramsey, chief technology officer for Dell SecureWorks. "Managed security service providers are necessary, because we are not going to solve these problems in the short term, and maybe not in the medium term either," he says. As more breaches expose more business and consumer information, cyber insurance has taken off. By 2025, the market will grow to more than twenty billion USD. However, policies continue to

have a large number of exceptions, leaving many firms to question whether the insurance companies will pay in the event of an incident. In May 2016, for example, CNA Financial Corporation sought a judge's ruling that the insurance company did not have to pay a little over four million USD to non-profit healthcare organization Cottage Healthy Systems (CHS). The lawsuit claims that CHS, or a third-party storage provider, failed "to follow minimum required practices", leaving data accessible to the Internet and unencrypted. Buying an insurance policy, therefore, (although alluring) may not excuse a business from obligations to reasonably protect its data.

2.3 The growth of the Internet of Things and complexity of industrial control systems will lead to more vulnerabilities in hardware systems.

Connected devices are becoming a greater part of our lives. From exercise-tracking devices to smart watches to sensors for monitoring industrial processes, business and consumers are using connected devices— the so-called "Internet of Things" or IoT— to collect information from the world around them and manage their lives and businesses. The Internet of Things will become such a part of our lives that people "won't even sense it, it will be all around you," Google ex-CEO Eric Schmidt told the World Economic Forum in Davos, Switzerland, in January 2016. Yet attackers are increasingly looking for vulnerabilities in both the IoT and industrial control systems to gain access to targeted data and systems. A variety of research into home automation and wearable sensors have spotlighted problems for consumer devices, with studies from Hewlett-Packard, Symantec and IOActive finding serious security issues in consumer devices, automotive systems, and home-automation systems. With devices and sensors finding their way into every industry and aspect of consumers' lives, security needs to become a higher priority. We are seeing the same thing with other physical systems— Transportation, health systems, robotics— everything is converted into the cyber-domain and that increases the number of entry points for attack.

Growth of Internet of Things and proliferation of mobile devices leads to a larger attack surface.

The number of connected devices and sensors is exploding. In 2007, excluding smartphones, approximately ten million sensors and devices communicated over a network. Currently, an estimated five billion such devices are now connected— a number that will continue to dramatically climb over the next decade, although estimates vary from twenty-five billion or fifty billion by 2020 to one trillion devices by 2025. The explosion in the number of devices has not resulted in manufacturers paying much attention to security. A small-sample study in Hewlett-Packard found that 7 out of 10 tested devices— including a smart TV, home thermostat and connected door lock— had serious vulnerabilities that could be attacked. A 2014 study by Symantec found that a seventy-five USD scanner could capture private or sensitive information from exercise trackers and other wearable devices. No one wants to build security into their devices, because no one is going to pay more for a secure device. So device manufacturers do not naturally have security in their mind set, which leads to an engineering staff that is not properly trained. There is so much focus on getting a product out the door that security is not a focus among the developers, so security has to be built in at design, or the update cycle needs to

be created to make the devices field upgradable. Yet, coming up with a single approach to improve the security of the Internet of Things is difficult, and currently the best way to secure devices is for the manufacturer or concerned customers to audit devices to ensure that. Industrial control systems (ICS) are a growing focus of vulnerability research and attacks. With such systems being used in a wider variety of settings, mitigating the vulnerabilities will become increasingly important. A few decades ago, industrial control systems were fairly limited, but now their functionality is expanding and they are being applied to new applications, such as home automation. We are moving in a direction now, where the only things not in the cyber domain are the analog parts of an actual physical system. Assessing the security of industrial control systems today often takes the form of a 'penetration test' that requires someone familiar with security practices, reverse engineering, real-world exploitation and the intricacies of a particular industrial domain. All of that is rare in a single team or person, so an end-to-end system is typically constructed to automatically detect and adapt inside new systems and networks.

As devices, systems and appliances increasingly communicate, verifying trust becomes a fundamental problem. Smartphones, which have become the mobile hub of people's lives, must have ways to determine how trustworthy, for example, a fitness band or a wireless speaker might be. Home routers or automation hubs will have to determine whether they trust a new security camera or an intelligent thermostat. While humans learn how to determine if another person or thing is trustworthy— based on information gained through perception, memory and context— whether those concepts can be transferred to the digital realm is still an active area of research. Machine-to-machine (M2M) trust is increasingly important, rather than trusting the channel through which machines communicate with one another.

The issues will become even more critical as digital technologies become an increasing part of our lives, such as some technologists' dreams of self-driving cars. Such vehicles will have to communicate with each other and be able to distinguish spoofed communications or illogical commands. All of this has to be done automatically without human intervention. Communication channels are going to be intermittent, so they will need to operate with resilience— you might trust the car next to you a little less if you know it hasn't been updated with the latest software patches. Today, trusting hardware, devices and data boils down to establishing a chain of trust, from the provider of the device or data to the method of delivery to the administrator of the asset. Each step requires verification, vigilance and the ability to detect changes to processes or devices. In the physical world, those activities have to be audited to ensure only trusted parties are handling the device or data. In the digital world, trust is established through digital certificates, encryption and other information-security technologies. Yet, weaknesses in this infrastructure are apparent. About 4.4% of all malware is signed using developer certificates as a way to circumvent and domain registrars have often been fooled into issuing fake online certificates. Even established Internet service providers can be fooled by weaknesses in routing protocols that make it possible for malicious actors to hijack traffic. The need of the hour, therefore, is a means to verify the true owner of a network and validate the international chain of

legitimate network paths redefining internet routing protocols as we know them. To protect critical cyber-physical system processes, a technology called Trustworthy Autonomic Interface Guardian Architecture (TAIGA) was developed to establish trust at the embedded-control level. The architecture creates a small root of trust that sits between physical processes and an embedded controller and maintains known good states. The code for the device is so small, it can be formally verified, and has been implemented in hardware, which has proved to provide additional performance and security benefits.

2.4 With few penalties if they are caught, nations continue to conduct online operations to steal information and gain advantage over their rivals, causing real economic impact.

In December 2015, a breach of the U.S. Office of Personnel Management (OPM)'s networks resulted in the loss of the digital files documenting background checks on all current and potential federal employees and contractors. The administration named China as the perpetrator, making the breach arguably the worst data loss attributed to a nation-state to date. The internet has become an intelligence battleground for every nation seeking an advantage on their rivals, with the OPM breach being one among many of the latest attacks. Without an effective deterrence, the operations will continue to escalate. The digitization of physical data— such as fingerprints, iris scans, palm geometry and other biometrics— could lead to an increase in theft of these unique signatures. There is an opportunity to leverage this data and it is too early to tell whether the bigger impact will be for good (e.g. broad adoption of strong authentication) or evil (e.g. fraud and impersonation). If no way is found to deter cyber-espionage and cybercrime, the drag on future potential benefits to the economy could be significant— as much as ninety trillion USD in 2030, according to a report published by the Atlantic Council and The Zürich Insurance Group. While cybercrime continues to be the most prolific malicious activity on the internet, nations and groups operating on behalf of national interests continue to expand. A great deal of cyber-espionage activity is attributed to Chinese actors. Yet, groups affiliated with France, Israel, Iran, Russia, Syria, the United Kingdom and the United States have all been documented. Documents leaked in a breach of offensive-tools provider Hacking Team indicate that the company sold surveillance tools and services to intelligence services in Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE, among other nations. In addition to digging deeper into the details of potential targets, nations are increasingly focused on examining the weaknesses in critical infrastructure. In a study of the interest in Internet-exposed critical information systems, one security firm found that two-thirds of attacks on the fake systems came from Russia and China, and nearly half of all critical attacks came from China. Over the past five years, cyber operations have evolved from gathering competitive intelligence to focusing on more general information about people. Nations are not just going after the data anymore, they are trying to affect functionality. This threat is especially relevant to embedded systems, which typically contain little protections yet often serve critical functions. Safety will, therefore, be a key driver of progress in the cyber security of operational technology, such as industrial control systems. Attackers continue to seek ways to make their code harder to detect and analyze. Signing code using developer certificates is the accepted way for programmers to signal that

their applications are official. However, attackers frequently steal certificates and then use them to sign their own spyware and malicious code. A study by Intel Corporation's security arm found that 4.4 percent of attackers sign their code.

The reality for users and security professionals is that preventing attacks is increasingly difficult. In response, organizations are finding ways to blunt the impact of breaches with techniques such as deceptive networks or comprehensive encryption. Attackers are advancing in other ways as well. Nation-states are experimenting with disinformation campaigns by hiring armies of "trolls", as they like to call themselves, to spread propaganda on the internet. Unfortunately, there are no easy solutions for responding to nation-state espionage or cyber-attack. As long as governments are able to plausibly deny involvement, disincentives are limited. There is an ongoing debate on the need for a strong offence, but there is an uncertainty among policymakers about when and how to go about it. Geopolitical realities and the interconnected nature of the global economy dissuade Western nations from using the "soft" level of power, such as sanctions and embargoes.

Policymakers continue to debate what constitutes appropriate deterrence to attacks in cyberspace. Cyber deterrence may require the concurrent use of political, economic, diplomatic and military tools with the realistic goal not to stop attacks entirely, but instead to reduce the volatility and intensity of cyber operations in future conflicts.

In the absence of a strong deterrence strategy, information sharing becomes an important way to bolster defenses. Better intelligence sharing could help companies collaborate on defending against attacks, but only if a workable solution can be found. The quality of commercial threat intelligence has risen dramatically in the past two years, with companies such as iSight Partners, Cyvillance and Dell Secure Works offering a range of tailored threat intelligence products and other companies— such as ThreatConnect, AlienVault's Open Threat Exchange and HP's Threat Central— offering services to support collaboration between industry peers. To be most effective, threat intelligence should be consumed in three tiers. Tactical threat intelligence has to be easily shared, machine-to-machine, to avoid delays. Operational threat intelligence should be leveraged by corporate IT security analysts in a security operations centre (SOC). Strategic intelligence must be in the hands of senior decision-makers who are driving business operations and making resource decisions.

"Unfortunately, many companies just aren't ready for a robot information sharing program," says Michael Farrell, chief scientist for GTRI's Cyber Technology & Information Security Lab. "They know about it, and many are trying to ingest a feed or two, but few have the resources of Facebook of Google to devote to a program in which they also share out (publish) actionable information in a useable format." While the attribution of attacks is often described as an inexact science, with the possibility of attackers using misdirection to throw analysts off the trail, most security experts believe there have been few missteps. While technical analysis can suggest a perpetrator, most commercial offerings today derive attribution statements from a blend of manual analysis of forensic and circumstantial evidence. Perpetrators often leave behind traces of network and host-based activity that can be correlated with other open source intelligence

sources to paint a picture of what transpired. Attribution is an extremely difficult problem when the goal is 100 percent certainty and the methods used must be scientifically robust. We are, therefore, in need of bringing machine learning techniques to bear against large malware libraries, commercial and public traffic logs, open source indicators of compromise, and other data repositories, with the goal of leveraging results from multiple domains of evidence to provide the context necessary to reduce uncertainty in attack attribution.

3. Industry Insights

Cyber-attacks on businesses have become common, hammering home the IT security mantra, "It's not a question of *if* but *when* you'll be attacked." If you're running a distribution or transportation business, it's likely either you or someone you know will fall victim to a cyber-attack. One possibility is the random defacing of your company's webpage, costing you temporary embarrassment or reputational damage. A more meticulously planned attack could result in the theft of the company or employee credit card information. Either way, cyber-attacks are a growing concern for businesses, and now's a good time to take steps to prevent damage.

IT security professionals have struggled with selling IT-related security to upper management for years. Some managers view IT security as an unnecessary cost that doesn't add value. However, recent news coverage of the Target, Home Depot and other security breaches has shed light on the importance of protecting proprietary and customer data.

There isn't a single preventive solution for cyber-attacks; IT security requires a layered approach to achieve maximum protection.

- **Network security** – This is an essential for any business, since firewalls are the most common frontline network defense. Networks requiring a more advanced level of protection can use intrusion detection systems and intrusion prevention systems (IPS) to actively monitor network traffic and alert administrators and security professionals to potential attacks or actively prevent them.

- **Computer security** – Network protection isn't enough, so businesses must take additional measures to protect individual computers. Host-based intrusion detection systems can prevent attacks on PCs the same way an IPS defends the network. Attackers can use social engineering methods to gain direct access to individual computers. For example, executable files attached to emails or downloaded from external websites could open the door for an attack. Companies should install virus and malware scanners to detect the presence of such files. In addition, IT specialists can disable USB ports and optical drives to prevent external media from automatically executing files and giving an attacker access to the device.

- **Physical security** – Often overlooked, securing the physical premises is a must when considering IT security. Easily purchased devices such as Raspberry Pi can open your network to myriad issues. They go for just $35 and can be set up to grant remote access, siphon data or perform any number of malicious attacks. Other problematic software and devices include key loggers that can record a user's keystrokes, USB man-in-the-middle devices that can open remote shells and portable VPN devices that can appear as

innocuous as a power adapter while establishing a VPN tunnel back to the attacker. These malicious devices and software have one thing in common—their installation requires physical access to the premises. Limiting physical access to the network is the best method of stopping attackers from deploying these devices.

- **Employee training** – People are the weakest link in the security chain. However, properly trained employees can be as valuable as any firewall, IPS or email spam filter. Training, like the approach to IT security in general, should be multifaceted. Concise and easy-to-digest periodic emails can be a quick way to remind employees of potential dangers. At the beginning of group meetings, consider including a short IT security discussion on topics such as:
    - Methods of preventing spear-phishing, *e.g.*, never clicking on suspicious links or downloading files from unconfirmed sources
    - The dangers of plugging rogue devices into company computers, *e.g.*, a simple USB drive uploading a malicious payload or acting as a man-in-the-middle device
    - Encouraging open dialogue between IT and employees if they believe something doesn't seem right

A CEO scam is another common attack for distribution and transportation companies. Criminals research high-level executives' names, roles and responsibilities and then impersonate them, requesting a check or wire to a fraudulent account. A typical example is a CEO impersonator sending an urgent request to the chief financial officer or controller while the real CEO is traveling or on vacation.

Distribution and transportation companies also should consider enhancing their Incident Response (IR), Business Continuity (BC) or Disaster Recovery (DR) programs to cover their cyber security gaps. For example, a computer can get infected with crypto locker malware from email or internet use, in some cases even from visiting legitimate websites. Once inside the transportation company's network, the malware attacks the infected computer by encrypting files and generating a message urging the user to send a bitcoin payment in exchange for the encryption key that would prevent the loss of files. Transportation companies with well-thought-out IR, BC and DR programs are better prepared for such cyber threats and can recover faster.

Employee awareness can't be stressed enough. The industry is awash in examples of businesses that have become victims of email phishing attacks due to the lack of employee training. Some companies have experienced attempted wire transfer fraud, while others have lost tens of thousands of dollars over a simple but critical mistake. In some email phishing schemes, frauders compromise an email account and then ensure no messages can be received from it. The account holder then receives an email asking for a large sum of money to be wired. In cases like these, employee awareness is critical to detecting and preventing monetary loss.

Cyber security continues to be a hot-button topic for transportation and distribution companies. Understanding the threats is only half the battle—implementing prevention methods is the next necessary step. You can help prevent attackers from turning you into their next victim by working in a layered security approach that covers the network, individual devices, physical access and an in-depth security awareness program.

References:

[1]. IT Governance Ltd [GB],(2016) *ISO 27001 Global Report 2016*
[2]. Georgia Institute of Technology,(2015) *Emerging Cyber Threats Report for 2016*
[3]. Hewlett Packard, (2014) *Internet of Things Research Study: 2014 Report*

