LINK TECHNOLOGIES

Cyber Security – The Holistic Approach

My-Ngoc Nguyen, CISSP, GCIH, GPEN, QSA, MS MIS

The growing number of attacks on our cyber networks has become, in President Obama's words, "one of the most serious economic and national security threats our nation faces." Modern society is deeply reliant on the services and information readily available through cyberspace. Unfortunately, the technologies that enrich our professional and personal lives also empower those who would benefit from carrying out cyber-crime and the associated disruption to our way of life. This is why business and government leaders are emphasizing the need to make safeguarding and securing cyberspace a critical priority across the Nation. Recent numerous cyber-incidents demonstrate the high likelihood of wide-scale or high-consequence adverse cyber events that would cause harm to critical functions and services across the public and private sectors as well as impact national security, economic vitality, and public health and safety.

Read how Link Technologies can help your organization implement good cyber strategy, mitigate likely threats and implement active cyber defense in a holistic manner.

My-Ngoc (pronounced "Menop") Nguyen is the Executive Vice-President for Link Technologies. She is a seasoned practitioner and acknowledged leader in the field of cyber security across a broad range of industries. She specializes in helping companies and organizations embrace the rapid change and evolution of technology and adopt the latest trends, in a secure manner.

Introduction

Enterprises all over the globe are compromised by malicious hackers each day. Proprietary and sensitive information, account usernames and passwords, credit card numbers and a wealth of other valuable data are surreptitiously transferred across the network. The growing number of attacks on our cyber networks has become, in President Obama's words, "one of the most serious economic and national security threats our nation faces". Today with the large dependency of technology and cyberspace, the Nation faces a myriad of threats from criminals, including individual hackers and organized criminal groups, as well as technologically advanced nation-states. Individuals and well-organized groups exploit technical vulnerabilities to steal American intellectual property, personal information, and financial data. The increasing number and sophistication of these incidents has the potential to impact our economic competitiveness and threaten the public's ability to access and obtain basic services.

The emerging cyber threats require the engagement of the entire society—from government and law enforcement to the private sector and most importantly, members of the public —in order to address and prevent their occurrence. Government, non-governmental and private sector entities, as well as individuals, families, and communities must collaborate on ways to effectively reduce risk. Cyber security is a shared responsibility, and each of us has a role to play. That entails working across the federal government, partnering with the private sector, and empowering the general public to create a safe, secure, and resilient cyber environment, and promote cyber security knowledge and innovation.

The Problem

Modern society is deeply reliant on technology and the ubiquity of information and services that it provides through cyberspace. Unfortunately, technology also empowers those who would leverage the enrichment it brings to our professional and personal lives to gain profits or meet their underlying objectives depending on whether the source is from a hacktivist group or a nation-state.

With all the recent cyber security incidents and breaches, business and government leaders in the US, along with our allies, have deemed safeguarding and securing cyberspace a top priority. These incidents have demonstrated the high potential for wide-scale or high-consequence adverse cyber events that would cause harm to critical functions and services across the public and private sectors and impact national security, economic vitality, and public health and safety.

The growing number of attacks on our cyber networks has become, in President Obama's words, "one of the most serious economic and national security threats our nation faces".

As malicious actors use increasingly sophisticated tools, techniques, and procedures, and the volume and velocity of cyber incidents across the nation continue to grow:

- Critical infrastructure must protect against, and be resilient in the face of, advanced and persistent breaches, which could degrade or disrupt the basic services upon which we depend, and set the stage for more destructive attacks.
- Government agencies must guard against exploits, which may remove or corrupt sensitive data and interfere with the delivery of essential mission services.
- Large corporations, medium and small businesses, and nonprofit organizations face increasingly sophisticated intrusions targeting their intellectual property and personal information about their customers and clients. Their systems are commonly used as launch pads for larger scale attacks.

- Consumers are routinely at risk of identity theft to obtain unauthorized access to personal information at numerous points on the Internet.

Current Threats/Activities

Over the past five or so years, there has been a dramatic increase in sophisticated attacks against nearly every type of organization. Cyber-attacks, also known as the Advanced Persistent Threat (APT), have proven difficult to suppress. APT, now a common term, is used to not describe the attacks but rather the attackers who are advanced and persistent. These attackers continue to leverage simple methods with well-known and well-dated vulnerabilities to break into systems. Nation states and organized criminals mainly from Eastern Europe and Russia continue to steal proprietary information and financial data like credit card numbers resulting in millions of dollars of losses. Attacks from hacktivist groups and nation states on government, government contractors, and Fortune 500 companies like Sony PlayStation, RSA, and LinkedIn are becoming bolder and more frequent. Major security incidents such as the 2011 breach by hacktivist groups WikiLeaks and Anonymous, who disclosed millions of US classified documents to the public, and Stuxnet, a computer worm (discovered in June 2010) designed to damage the Iranian Nuclear Program, are examples of such bold attacks. Sophisticated hackers can advance rapidly through any individual networks using techniques and tactics such as spear phishing, web application attacks, and custom malware while using anti-forensic techniques to hide and cover their tracks. An external attack becomes an insider attack through the leverage of cutting-edge covert tunneling techniques which allows the export of data from highly secured environments while the attacker remains undetected for lengthy periods of time.

The section below captures some of the trends, tactics, and techniques of APT and emerging threats along with some recent security incidents and breaches.

Cyber-espionage that pose a potential threat to the nation

Flame and Stuxnet are two examples of security incidents that raise the Nation's concern of cyber-espionage. Flame is a malware that disguises itself as a legitimate file, sometimes masquerading as a routine Microsoft software update, and once installed, will replicate itself and spread through the inside of network systems. A Flame can "activate its [sic] microphones and cameras, monitor keyboard strokes by users, extract geological data from saved images, snap screen shots of working computers, and even send commands to other peripheral devices" mentions the Washington Post in an article about this particular virus.

Flame virus has been linked to the Stuxnet incident, which was created to gather information on Iran's nuclear program. Stuxnet was responsible for damaging hundreds of centrifuges at an Iranian nuclear facility, and it is believed to have slowed down the nation's nuclear program by an estimated two years. Many security experts in the nation now predict this might create a backlash and counter espionage strike that will be aimed towards businesses in the US and Israeli nations.

Malware Supermarkets: Making Cybercrime easier to commit.

The FBI has classified cyber crime a number one priority to combat, mainly because cyber crimes are easier to commit with the rising availability of easy-to-use malware kits, available through online black market networks, like the Tor network, which prevents its users with criminal intent from being tracked. Such malware, as the Blackhole Exploit Kit, Eyestye and Zbot, require very little effort or IT knowledge to use and are low-cost (less than $500).

An example of the use of malware-for-sale was reported early in April (2012). According to an *e-week.com* article, the USPS national support

center, *ribbs.usps.gov*, had fallen victim to hackers, who used the Blackhole Exploit Kit to inject a malicious Javascript that redirected the visitors to a different site. While the users saw a "404 Page Not Found" error message, there was a download in the background that injected various types of Trojans and several malicious PDF files and PHP scripts that went undetected by most major antivirus programs. The affected site, Rapid Information Bulletin Board System, handled the postal service's intelligent mail services, which catered to services like barcode-based tracking for business mail. One can only imagine the backlash and frustration to the users of this service with this security compromise. Therefore, with the availability of easy-to-use malware the chances of a security compromise are high and it is a challenge that organizations should counter measure with adequate preparation.

> …***cyber crimes are easier to commit with the rising availability of easy-to-use malware kits, available through online black market networks***

Banking Trojans: A Threat to Financial Institutions

A Trojan is a malicious file that once injected into a user's computer can make copies of it, steal information or provide software backdoors that can track the actions of the user. Phishing e-mails, which are e-mails containing links to these types of malware, are a growing trend in how Trojans are injected into a user's system.

According to Gordon M. Snow, Assistant Director of Cyber Division for the Federal Bureau of Investigations, in a testimony to the Subcommittee on Financial Institutions and Consumer Credit at Washington D.C., last September, Cyber threats to financial institutions will be a rising concern for the FBI, and potential regulation trends of security safe practices for financial institutions might be planned to mitigate some of the concerns to financial institutions.

An increasing trend in crime against financial institutions is account takeovers through security compromise. The exploitation of Internet-based commerce systems interfaces, card payments and market trades has led to fraudulent monetary transfers. A current investigation of over 400 cases involves theft of over $255 million. The attack vectors are through phishing e-mails that contain links to malware that is installed onto the users' computers, which include key logging programs to harvest the user's personally identifiable information (PII) subsequently enabling the criminal to transfer the user's funds. Among the several cases mentioned by Snow, one involved a school district in Pennsylvania, which had over $450,000 in fraudulent transfers, and another involved a school district in New York, which had over $3 million transferred out through these types of phishing attacks.

Mobile banking exploitation is another venue for Personally Identifiable Information to be compromised. Mobile phone attacks involve variations of ZeuS malware, that send phishing text messages with links that deceive the users into disclosing PII over their mobile devices. These types of attacks have enabled identity theft, compromised social security numbers, bank account information, and insider access to proprietary company data that proves these threats to be detrimental to those who are victimized by these attacks.

Cyber Crimes are well organized

A concern expressed by Microsoft's Trustworthy Computing (TwC) division experts is that cyber crime is being committed in a well-organized manner. There is a notable increase over the past two years, of cyber-crime from poorer economies that target other nations through online venues that also leverage very sophisticated anti-forensic techniques that hide their track. Some of the techniques utilized by hacktivist groups include rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware that

outsmart current file intrusion detection technologies utilized by most organizations. As cyber-crime sophistication, and its corresponding threat to industry increases, the notion that cyber-crime is a major concern to an organization's functionality and its global implications cannot be overstated.

Spam: bulk email that increase the occurrence of false positives

Spam is unsolicited bulk email for commercial purposes, which have with it associated anti-spam laws that make it unlawful in certain jurisdictions. Though spam is traditionally viewed as being harmless, it nevertheless hosts a venue for mal-ware to sneak into an organization's network if not mitigated properly. Spam mitigation raises concern for security experts because it contributes to the perception of false positives, or legitimate or harmless files being flagged as a malicious file by email security scanning systems. Too many false positives have the tendency for users to be lax about certain e-mails that could perhaps contain malicious files. Thus, Spam mitigation is a security issue that should be addressed properly by organizations.

Best Practice Considerations

Many believe that they are secured because they have a firewall and anti-virus installed. However, security is about defense in-depth. The first step to this is the continuous improvement of an organizations' cyber security posture and enhancement of their cyber security best practices. Secondly, to deter and mitigate threats, organizations must strengthen their workforce communications, workforce accountability, internal monitoring, and information management capabilities. Third, organizations must employ an active cyber defense capability to prevent intrusions into their networks and systems. Fourth, organizations, including government, need to continue to develop new defense operating concepts and computing architectures. All of these components combine to form an adaptive and dynamic defense of networks and systems.

Most vulnerabilities of organizations' systems, and therefore malicious acts against them, can be addressed through good cyber defense. Cyber defense must be practiced by everyone at all times; it is just as important for individuals to be focused on protecting themselves as it is to keep security software and operating systems up to date. Further, good cyber defense extends to the maintenance of information security, the promotion of good cyber security practices for users and administrators alike, secure network design and implementation, and the employment of smart and effective network and configuration management. This holistic effort will provide protection, monitoring, maintenance, design, and care for an organizations' networks and systems to assure their security and integrity.

People are the organization's first line of defense in sustaining good cyber security and reducing insider threats, especially those that are originally external threats. Organizations must seek to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity. This cultural shift needs to be enabled by new policies, new methods of personnel training, and innovative workforce communications.

As malicious cyber activity continues to grow, there is a need to employ active cyber defense to prevent intrusions and defeat adversary activities on networks and systems. Active cyber defense provides an organization with synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It must build on traditional approaches to defending networks and systems, supplementing best practices with new operating concepts. The defense must operate at network speed through the use of sensors, software, and intelligence to detect and stop malicious activity before it can affect networks and systems.

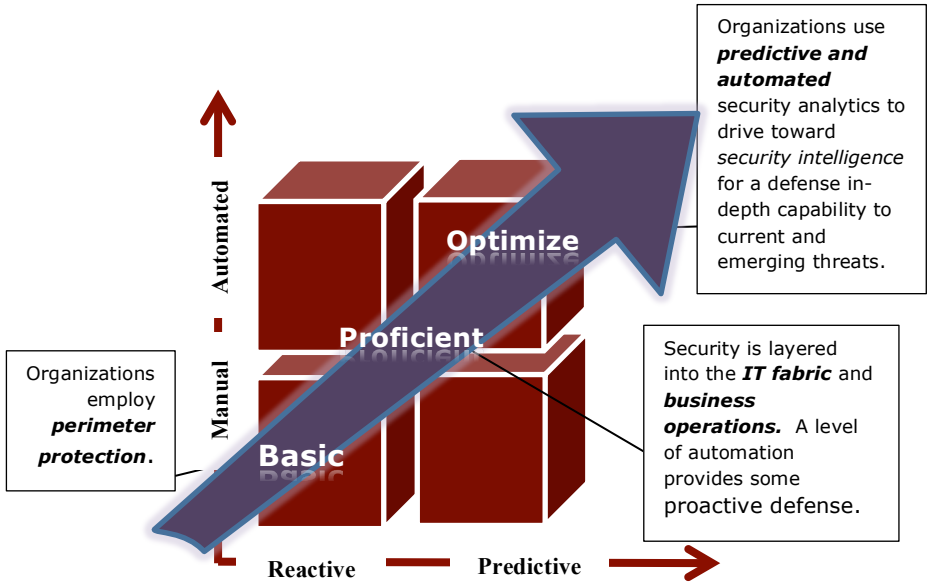
To foster resiliency and smart diversity in networks and systems, organizations need to explore new and innovative approaches and paradigms for both existing and emerging challenges. These efforts will include development and integration in the areas of mobile media and secure cloud computing. Organizations need to continue to be adaptive in their cyberspace efforts while embracing both evolutionary and rapid change with the integration of security.

Link Technologies Value Proposition

In the last couple of years, it has become obvious that, in the world of information security, the offense is outperforming the defense. Even though budgets increase and management pays more attention to the risks of data loss and system penetration, data is still being lost and systems are still being penetrated. Over and over people are asking, "What can we practically do to protect our information and information systems?"

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. In addition, Link Technologies is an active member of threat intelligence groups (e.g. FBI, Counterintelligence) and a leading research institute (i.e. SANS), which provide knowledge of emerging threats. With leading knowledge of the threat landscape, the recommendations and guidance we provide integrates a full risk perspective that enables organizations to prioritize and focus on key security investments and initiatives.

Link Technologies, with our depth of expertise and rich experience related to the entire cyber security lifecycle have solutions designed to protect and secure your information assets, provide integrated security management services, reduce risk, and meet compliance objectives. Link Technologies offers an industry best practices approach based on our extensive portfolio of cyber security and information assurance services, as well as proven leadership in providing cyber security solutions for high-profile clients. Link Technologies is experienced with all the federal laws, and regulations that apply to cyber security and privacy such as FISMA, SOX or PCI compliancy guidelines.



<u>Our solutions can assist organizations mature from basic to optimized</u>

Link Technologies' cyber security planning development approach ensures harmonization with organizational culture, mission, and business requirements, as well as relevant laws and regulations. Our approach focuses on establishing and maintaining relationships with the system owners to develop and update

planning documentation that reflects current operational needs, requirements, threats and government cyber security directives.

We provide our insights, lessons learned, experience and technical capability to provide cyber security protection, planning and risk management services for the future.

We are proud of our comprehensive, systematic set of processes to identify and seamlessly mitigate vulnerabilities, including those associated with out-of-date software and firmware which allows an IT organization to maintain the availability, authenticity, confidentiality, and integrity of the systems they support. Link Technologies is vendor agnostic as we review technology and tools via a disciplined process that addresses and balances tool effectiveness, security, cost, ease of use, and customization/integration abilities and efforts. Link Technologies values the need for a suite of security tools as an essential element to incident management (i.e. prevention, response, and handling). Because there are no be-all and end-all solutions, we emphasize the importance of having an expert staff to manage a portfolio of security tools with disciplined engineering and tuning.

For more information on how Link Technologies can help you improve your information security posture visit **www.linktechconsulting.com** or call us on **(702)233-8703**. Let us help you adopt and implement evolving technologies, with the integration of security as a foremost guiding principle.

Creative Solutions for the Next Generation of Technology.

Link Technologies is a certified 8(a), SDB, WOSB, and DBE small business founded in 2000. We built an outstanding reputation for client-focused performance and for delivering results that enable clients to meet commitments and milestones.

The Link Technologies team is carefully selected to include only experienced and well-qualified individuals. This team offers a suite of core capabilities to address the specific needs of our clients and deliver innovative, timely, and cost effective solutions.

The highly qualified staff and Subject Matter Experts at Link Technologies hold top level certifications and degrees.

Contact My-Ngoc Nguyen •
MyNgocN@LinkTechConsulting.com

Federal ID: 68-0510468
DUNS: 118034169
CAGE Code: 3A1V1
WBENC: 2005111754
Primary NAICS Codes:
541330, 541511, 541512
541990, 541690, 541519
SIC Codes: 8742, 7373, 7379, 7371
Registrations: CCR and ORCA
Certifications: