December 2013 / Issue 27

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Looking Ahead at 2014

Predictions are surfacing about what we can expect to see regarding cyber security in 2014, as greater pressure for compliance and adherence to national standards such as the updated NIST cyber security framework emerge.

According to the Information Security Forum, key threats for 2014 include bring your own (BYO) device trends in the workplace, data privacy in the cloud, brand reputational damage, privacy and regulation, cybercrime, and the continued expansion of ubiquitous technology. As attacks become more sophisticated and while organizations try to develop new techniques to prevent them, cyber criminals will be working on ways to circumvent those techniques. Other organizations like WatchGuard Technologies predict advances in ransomware, hacking of IoT (Internet of Things) devices, critical infrastructure exploits, and a data breach of HealthCare.gov. With online privacy concerns expected to take center stage, both Symantec and McAfee said they expect to see more threats from mobile apps for smartphones in 2014 and that consumers should be aware of what they could be consenting to when they download an app.

Trend Micro's annual security predictions report, "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond," suggests that "one major data breach will occur every month next year, and advanced mobile banking and targeted attacks will accelerate." The Android operating systems is expected to see increased instances of malware, with some IT experts predicting the total number of malicious and high-risk apps to reach three million.

2014 will prove to be a challenging year in cyber security. The "insider threat" continues to remain prevalent and we are beginning to see businesses and governments worldwide making efforts to bolster their cyber programs. And since Microsoft is dropping support for Windows XP in April, we can also expect to see hackers preying on XP vulnerabilities—that means that the 20 percent of computers still running it as well as many ATMs will be at risk if they don't update (Trend Micro).

As always with cyber security, have a plan, take action, monitor, and be vigilant. Happy New Year!

December 2013
Cyber Attack Statistics
- **Hackmageddon.com**

Attack Motivations
- 45% Hacktivism
- 53% Cyber Crime
- 1% Cyber Espionage

Top 3 Attack Targets
- 30% Government
- 25% Industry
- 5% Organization

Top 5 Attack Techniques
- 30% Defacement
- 23% Unknown
- 10% Account Hijacking
- 15% DDoS
- 4% SQL

Industry News

IT under threat from "major" cyber attacks

From www.scmagazineuk.com, 12/17/2013

IT departments are short on time and security tools, and are under more threat than ever before, according to a new report. In a study of 350 IT professionals in the UK, security management solution provider RedSeal Networks found that a significant number of professionals felt under-resourced, short on time, and subsequently were ignoring 'critical' security vulnerabilities and fearing 'massive' cyber attacks. Approximately 30 percent of IT departments admitted to turning a blind eye to critical security vulnerabilities because they didn't have the time or tools to get to the root of the problem, while 28 percent pleaded for more sophisticated tools to manage the deluge of data. Another 41 percent also said that they feared a major cyber attack against the UK's critical national infrastructure. As such, a number of IT departments were unconvinced if their networks are secure, or even confident that they could pinpoint a cyber attack.

Imperial institute to study cyber threat, hopes to prevent industrial control system hacks

From www.tcetoday.com, 12/17/2013

A new research institute is to be set up at Imperial College London to investigate potential cyber threats to industrial control systems. Industrial control systems include components such as computer hardware, software, mechanical parts and sensors, and are important for all kinds of infrastructure, including manufacturing, nuclear power generation, energy distribution and even rail networks. Increasingly, industrial control systems are connected to the internet through business IT networks, rather than operating in isolation, leaving them more open to attack. In addition, many such systems must operate continually, so finding time for a shutdown to first vigorously test and then install upgrades and patches to prevent a cyber attack is difficult.

Defense bill protects Delaware cyber security unit

From www.washingtonpost.com, 12/20/2013

A defense bill passed by Congress includes a provision to protect funding for a Delaware National Guard cyber security unit. U.S. Sen. Chris Coons says language he included in the bill will protect the New Castle-based 166th Network Warfare Squadron. Coons says the squadron helps protect America's critical infrastructure systems against the threat of cyber attacks, and that language in the bill would halt and likely prevent cuts to the squadron, as well as cyber units across the Air National Guard.

Water utility sector works in partnership to meet cyber security challenges

From www.huffingtonpost.com, 12/5/2013

The nation's cyber security-related consciousness has steadily grown as we have become more aware of the unintended vulnerabilities that leveraging enhanced technologies like ICS can bring. This is not just a private sector issue. The federal government, which uses cyber technologies, has given this matter significant attention as of late. Most recently, President Obama designated November 2013 as "Critical Infrastructure Security and Resilience Month," with the intention of recognizing the importance of protecting our nation's critical cyber systems and encouraging activities that enhance security and resilience. Simply put, through cyber security-related programs and initiatives, the public and private sectors are coming together to provide a secure network that safeguards the critical infrastructure systems America relies on, including those that distribute and transmit water, electric power and gas services. The solutions yielded via this partnership are composed of a combination of key capabilities that include implementing physical and virtual security measures. These range from the establishment of virtual private networks (VPN), the institution of firewalls and routers to control network communication and prevent unwanted traffic, to promoting basic computer safeguarding protocols like enhanced computer password protections and limiting user access to sensitive networks.

Energy industry is on alert against increasing cyber attacks

From www.ffw.com, 12/2/2013

Governments the world over have been ramping up their digital agendas in recent months, each seeking to instill the importance of cyber security on citizens and businesses alike. Attempts are being made to raise cyber security awareness, and essentially the message is that organizations must understand their networks, systems and data, and must take a proportionate, risk-based approach to keeping them secure. Resilient networks and systems must be in place. This is especially important in the energy industry, which has become increasingly vulnerable to cyber attacks by 'hacktivists', state-sponsored hackers and other cyber criminals who are all seeking to exploit network and system vulnerabilities.

Cyber News

Target credit card data theft shows everything is hackable

From www.boston.com, 12/20/2013

The news that 40 million Target customers' credit and debit card accounts may have been revealed to cyber criminals who gained access to the store's payment card data highlights a simple and uncomfortable fact: American companies are lagging behind the hackers who are intent on stealing their data and disrupting their operations. As cyber attackers grow in number, capability, and sophistication, firms must ensure that their security systems and procedures keep pace. Improving cyber security isn't a challenge solely for intelligence agencies and the Department of Homeland Security. Only about 10 percent of America's critical infrastructure is owned by the government. And while programs like DHS's Enhanced Cyber Security program are ramping up to share threat intelligence for critical infrastructure, the private sector also has to take responsibility for protecting its systems against attacks as well.

Stock exchanges of the world band together to repel cyber attacks

From www.tgdaily.com, 12/19/2013

The World Federation of Exchanges (WFE) announced the launch of the exchange industry's first cyber security committee. The committee is tasked to combat systemic cyber abuse against world capital markets. The Cyber Security Working Group will be chaired by Mark Graff, Chief Information Security Officer, NASDAQ OMX and vice-chaired by Jerry Perullo, Vice President, Information Security, IntercontinentalExchange (ICE). "The creation of this committee group is a significant milestone for the global exchange community," said Ravi Narain, Chairman of the Working Committee. "Cyber security is a crucial issue to global markets, and paramount for maintaining market integrity and resiliency. We are pleased with the positive collaboration in this committee, which will transcend competitors and regions in order to tackle key issues and present best practices, and we believe that the formation will universally benefit the financial markets of the world."

Cyber attack probe inconclusive

From www.japantimes.co.jp, 12/20/2013

The Metropolitan Police Department has decided to end its investigation of a cyber attack against Mitsubishi Heavy Industries Ltd., Japan's biggest defense contractor, before the three-year statute of limitations expires. This shows how difficult it is to investigate crimes committed in cyberspace. It must be kept in mind that any company or organization throughout the nation can be the target of a cyber attack and that precautionary measures should be taken. In the attack on MHI, 45 servers and 38 personal computers at its Tokyo headquarters and at 10 other sites for manufacturing and research and development were infected with eight kinds of viruses. The viruses connected the Mitsubishi servers and computers to servers overseas for the purpose of hacking information. MHI says there were no leaks of protected information.

Defense to weigh civilian cyber militia

From www.nextgov.com, 12/20/2013

Congress has mandated that Defense Secretary Chuck Hagel evaluate the practicality of hiring part-time nonmilitary employees to help the National Guard thwart cyber attacks. Some states and other nations, including Estonia, already have volunteer netwarfare squads poised to protect networks controlling oil reserves, subways, and other critical infrastructure in times of crisis. The corps outlined in the 2014 National Defense Authorization Act that lawmakers approved on Thursday night would recruit "non-dual technicians," or National Guard personnel who are not required to deploy overseas. Dual-status employees must be uniformed military members and maintain their Defense Department ranks and assignment units.

Young professionals exposing workplaces to cyber attack

From www.net-security.org, 12/12/2013

Low cyber threat awareness amongst Gen-Y professionals coupled with blasé attitudes towards cyber security are leaving organizations across the country exposed to attack and data leaks according to ESET. Thirty-eight percent of Gen-Y professionals, those aged 18 to 30 years old, are unaware of, or don't believe, their company has an IT security policy, whilst a further 30 percent of those who are aware of the existence of an IT security policy do not know what it is. Half also believe it's nearly always their organization's sole responsibility to ensure the safety of data.

Consultant's Corner

Centralized Management with Active Directory

Managing servers, users, accounts, and security policies is critical to the overall security of your system. Performing these tasks locally on each machine is inefficient and leads to higher administrative costs. Inconsistent local management may introduce vulnerabilities and lead to inconsistent security policies.

Active Directory provides a variety of functions that enhance centralized management:

- **Centralized user accounts** — Active Directory provides an efficient way to store and manage your user accounts.
- **Centralized policy management** — Through Active Directory, you can centralize the definition, management, and deployment of security policies that safeguard each according to the role that each server plays.
- **Centralized security model** — Active Directory provides a security model that defines roles for the accounts together with restricted rights associated with these roles. Active Directory is also a solution for locking down various critical objects in the environment to ensure that the security model cannot be violated.

The centralized security model allows you to create and manage server and user privileges, authentication, and security within your environment more efficiently than managing them locally on each server. Without a way to manage servers centrally, someone must manually configure security settings, perform updates, manage users, and perform other manual maintenance tasks. The centralized security model dramatically reduces operational complexity, improves security, and lowers risk through consistent policy application.

There are a number of significant server management benefits delivered by centralized management:

- **Simplicity** — A powerful yet simple model that DCS staff can use for managing user accounts and associated rights, eliminating the confusion that exists when each server maintains accounts and passwords locally.
- **One set of tools** — Because you define all accounts and rights in a single, central location using Active Directory, you can use one set of tools to manage the solution. The centralized management solution provides internal tools that directly access and manage Active Directory.
- **Global security policy** — Your organization can also realize operational benefits through defining and managing a global security policy, including security lockdown processes. The security policy is clear and simple, as opposed to the inevitable confusion that occurs when each server has its own security details.
- **Automatic deployment of security policies** — Centralized security permits you to deploy security policies globally from a central source to each server. Centralized deployment of security policies minimizes the disadvantages associated with manually applying security lockdown.
- **Efficiencies in security** — Your organization realizes cost efficiencies and reduces operational tasks because any additions or changes to the overall security policies are implemented only once in a centralized location.

A centralized management infrastructure enables you to create and manage server and user privileges, authentication, and security within your network more efficiently than a local management implementation. Incorporating Active Directory in your system provides a centralized solution for managing servers and users. For server management, Active Directory provides a single point of management for all user accounts and associated rights for your staff.

This month's contributor to Consultant's Corner is
Chad Dunaway
Consultant, Critical Infrastructure & Security Practice, Invensys
chad.dunaway@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
December 2013 / Issue 27

Invensys Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements and company compliance requirements. Attributes of Invensys CISP Critical Infrastructure Consulting include:

Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as active participation in a number of industry and government groups.

Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

Join us on Blogger

Industry Knowledge

CISP has a number of resources that understand the demands of Controls Networks and the requirements for continued uptime.

Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessments, Development, Implement and Management.

invensys

For additional information, please visit us at
http://iom.invensys.com/CyberSecurity

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**