The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

October 2014
Issue 37

this issue

How cyber security impacts the physical security world

From us.sourcesecurity.com, 10/1/14

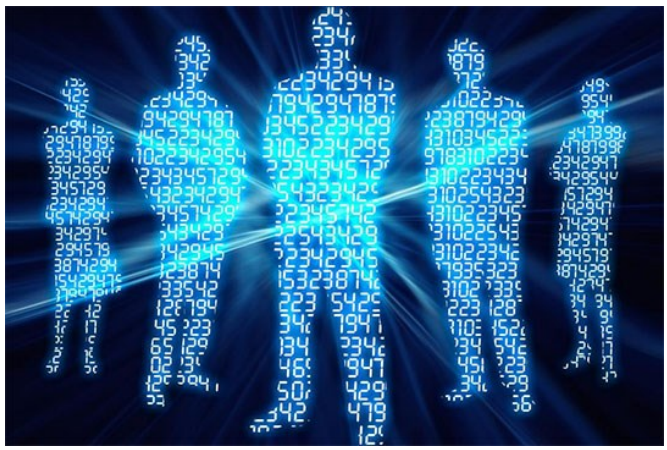
The physical security market tends to dismiss issues of cybersecurity as outside its area of expertise, but cyber-threats are a problem that has been ignored for too long. The fact is, cybersecurity is a critically important aspect of the systems our industry provides in the increasingly IP-driven world of physical security. PSA Security Network is seeking to raise awareness of cybersecurity in the physical security world, and to highlight possible business opportunities for security integrators in cybersecurity. Goals include getting the communities together and making sure physical security integrators know the risks and the solutions that cybersecurity has to offer, says Bozeman. Another goal is to make sure cybersecurity companies understand the physical security integrator's needs. "Physical security cannot just sit there and do nothing," says Bozeman.

The Insider Threat

While many companies are focused on securing their networks and intellectual property from external cyber security threats and attacks, an often overlooked danger is the threat from within. Employees with privileged access rights to systems can easily manipulate and compromise their security, whether intentional or not, and cost companies billions of dollars. Other factors such as negligence, sub-contractors, theft of trade secrets, and mobile media can all contribute to the insider threat. According to an IT Governance survey, "only 27.4% of reported breaches were known to be attributable to external threats," with the remaining two-thirds of attacks linked to the inside.

Last year in the US alone, companies and organizations that fell victim to insider attacks lost a total of around $40 billion (SpectorSoft Corp.), and 54 percent of organizations believe "it is more difficult to detect and prevent insider attacks today than it was in 2011" (www.baselinemag.com). A report from Kroll Advisory Solutions suggests that "moles, opportunists, contractors, disgruntled employees, and ex-IT personnel—all currently pose a greater risk to corporate intellectual property than state-sponsored hacking and APTs, both in frequency and in damage caused."

So what steps can companies take to protect their assets from insider threats? For starters, they can improve their employee profiling to identify those who may commit these types of crimes. According to CSO Magazine's 2012 CyberSecurity Watch Survey, "organizations that experienced cybercrime by an insider in the previous 12 months reported that 51 percent of those insiders violated IT security policies and 19 percent were flagged by a manager for behavior/performance issues." Additionally, stricter termination policies should be in place that immediately revoke access rights of terminated employees, and internal network monitoring and log retention can go a long way in preventing insider threats. Even if criminal activity surfaces, retaining logs of network activity can make investigations easier if information is organized, maintained, and secured in one location.



The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2014 / Issue 37

Industry News

Security firms tie Russian government to utilities hacks

From www.businessweek.com, 10/30/14

North American utilities are scouring their systems for signs of Russian malware that the U.S. government has warned could give hackers control of water treatment facilities and parts of the electrical grid. The U.S. Department of Homeland Security issued alerts about digital attacks on utility computer systems on Oct. 8, Oct. 17 and Oct. 28. The agency didn't identify the country behind the hacks, but cybersecurity firms yesterday connected them to Russia. The firms have cautioned in recent reports that cyberspying by Russia is on the rise, and a recent breach of an unclassified White House computer system was linked to the Russian government or criminal hackers.

Cyber attacks most imminent threat to U.S., economy

From www.threatpost.com, 10/28/14

In a panel discussion this month, a crowded table of top-level security experts from industry, military and government agreed that the threat posed by cyber attacks targeting U.S. critical infrastructure and private industry now outweighs any other national security threat. Problematically, the government will not and cannot solve that problem alone. Private companies will have to look within and to each other and partner with the government if they want to protect themselves and, more broadly, U.S. interests, the experts said. The goal for securing networks, the panel would agree, is not one of preventing attacks altogether, but accepting that networks will be breached and aiming to limit the amount of time that an adversary spends within a compromised network.

CompTIA adopts federal framework for cyber security

From thehill.com, 10/27/14

The major IT industry group CompTIA has tweaked its security certification program to match the National Institute of Standards and Technology (NIST) cyber security framework. CompTIA has board members from Comcast, Dell, Hewlett-Packard and Xerox. Its CompTIA Security Trustmark+ program evaluates companies' cybersecurity architecture. "We've strengthened the underpinnings of the Trustmark so that it aligns with other rigorous security compliance standards," said Nancy Hammervik, CompTIA senior vice president for industry relations.

Ex-Homeland Security Chief says energy industry under increasing threat of cyber attack

From naturalgasintel.com, 10/1/14

Former Department of Homeland Security Secretary Tom Ridge told an oil and gas industry audience in Pittsburgh that digital security should be a top priority at their companies, adding that current policies are outdated and the threat of cyber attacks grows by the day. Ridge, a Republican who also served as Pennsylvania's 43rd governor, said natural disasters, terrorists and foreign countries are among the leading threats to the intricate industrial control systems used by exploration and production companies, midstream operators and suppliers. He said with oil and gas development at the forefront of the country's economic recovery, and with billions more devices and users expected to come online in the year's ahead, the industry should be taking extra caution to protect proprietary information and its link to national security.

India asked to join global cybercrime control initiative

From indiatimes.com, 10/18/14

The Netherlands has asked India to join in an international initiative for capacity building in the area cybercrime control to be launched in April next year. The initiative is to be launched at the fourth Global Cyberspace Conference to be hosted by Netherlands during April 2015, Uri Rosenthal, the country's special envoy for the conference, told reporters Friday on the sidelines of a conference here on cybersecurity and governance. "We have discussed with the Indian foreign ministry for getting India on board in the initiative we'll be launching for capacity building in April," said Rosenthal, who was earlier the Dutch foreign minister.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2014 / Issue 37

Cyber News

Singapore: Attacks driving growth of cyber security, analysts say

From http://www.businessinsurance.com, 10/2/14

The Economic Development Board and the Infocomm Development Authority of Singapore have said that the country's favorable business market have attracted cyber security firms to set up shop in island nation, reports Channel NewsAsia. Analysts have said that cyber attacks are one of the significant factors driving the growth of cyber security industry in Singapore. The cyber security industry in the Asia-Pacific region is expected to grow about 13.4% annually, touching $26 billion by 2017.

Suspicious cyber activity detected at the White House

From www.securityweek.com, 10/29/14

White House technicians recently detected suspicious activity on a computer network at the US presidential mansion, and have taken steps to resolve the issue, an official said. The White House official said the Executive Office of the President receives daily alerts concerning numerous possible cyber threats. "In the course of assessing recent threats, we identified activity of concern on the unclassified EOP network," the official said. "Any such activity is something we take very seriously. In this case, we took immediate measures to evaluate and mitigate the activity."

'Major' hacking attack in U.S. looms

From www.securityweek.com, 10/29/14

Cyber attacks might be taking a toll now, but just wait: a survey of experts says things are likely to get even worse in the US over the next decade. A majority of cyber security experts surveyed in a poll see a likelihood of major damage from a cyber attack in the coming years, according to a Pew Research Center report. From the 1,600 experts polled, 61 percent answered "yes" to the question: "By 2025, will a major cyber attack have caused widespread harm to a nation's security and capacity to defend itself and its people?"

Biggest ever cyber security exercise in Europe is underway

From www.net-security.org, 10/30/14

More than 200 organizations and 400 cyber-security professionals from 29 European countries are testing their readiness to counter cyber attacks in a day-long simulation, organized by the European Network and Information Security Agency (ENISA). In CyberEurope2014, experts from the public and private sectors including cyber security agencies, national Computer Emergency Response Teams, ministries, telecoms companies, energy companies, financial institutions and internet service providers are testing their procedures and capabilities against in a life-like, large-scale cyber security scenario.

Global cyber attacks up 48% in 2014

From www.cgma.org, 10/8/14

Security incidents cost businesses an average of $2.7 million each year, according to a survey by PwC. Despite the burgeoning threat, information security is an issue that receives little involvement from the board, and security budgets decreased in the last year. The Global State of Information Security Survey 2015 was conducted by PwC, gathering responses from more than 9,700 security, IT, and business executives in 154 countries. The research found that the number of detected information security incidents has risen 66% year over year since 2009. In the 2014 survey, the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48% from 2013—an average of 117,339 per day.

Cost of cyber attacks jumps for U.S. firms

From www.securityweek.com, 10/16/14

A survey of 59 US firms by the Ponemon Institute with Hewlett-Packard found the average annual cost of responding to cyber attacks was $12.7 million, up 96 percent over the previous five years. The organizations saw a 176 percent increase in the number of cyber attacks, with an average of 138 successful attacks per week, compared to 50 attacks per week when the study was initially conducted in 2010. The average time to detect an attack was 170 days, and it took on average 45 days to resolve a cyber incident, costing an average of $1.6 million, according to the researchers. The costs of cyber attacks include detection and data recovery, as well as loss of information and disruption to business, the report said.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2014 / Issue 37

What Should I Protect?

When implementing a cyber security program, many people tend to get lost in how to prioritize what to protect. The massive number of systems in an industrial control system and their potential interaction with the outside corporate and public world seems daunting. Many articles on the internet direct everyone to use a risk management approach, but many people tasked with establishing a cyber security program serve an operational role in either the ICS or IT department. Risk management may not have a logical meaning for them. They may view that everything that they deal with operationally is vital to company business and has to be protected at the same level.

Another term that is sometimes difficult to understand is "defense-in-depth." Some people may think that means bury that important industrial system under every defense method imaginable. But in some cases, that assumption is not always true.

Imagine if you were trying to defend a small town in medieval times. Would you set up a wall and moat around each critical part of town individually? Would a trash pile in town be worthy of protecting?

On the other hand, would you put a wall and moat around the town, but put the king and queen in a straw hut right next to the wall? If any of your "walls" get breached, do you just raise the "white flag" and surrender? What if crossing the first "wall" of your defense leads to a moat that traps the enemy?

Through these illustrations, you begin to understand what risk management and defense-in-depth really mean. Risk management is all about determining what systems are **really** important to your business based on the roles they serve and data they provide. A popular question when performing risk management on a system is "Can I live without this system for 5 minutes? 30 minutes? Hours? Days? Weeks?" Based on how you answer this question, it will determine the number of defense-in-depth methods you need.

In planning your cyber security program, is it realistic to think you can reduce your risk to zero by layering enough defenses? Many industry trends show that just one weak defense can bring down an entire cyber security program. So is all of this "cyber security" worth it?

Cyber security is worth the investment, but many people need to shift their paradigm to realize the following: you may have already been compromised. Once you realize this, your cyber security program becomes less about how to keep the bad guys out, but more about "how do we detect when they are here? What do we do with the bad guys when we have discovered them?"

This month's contributor to Consultant's Corner is Charles Smith
Consultant, Critical Infrastructure & Security Practice, Invensys
charles.smith@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2014 / Issue 37

Most Popular Blog Posts This Month

Cyber attacks an increasing threat for Mideast oil and gas (October 17, 2014)
Cyber attacks are increasingly becoming a cause for concern for oil and gas companies operating in the Middle East, information technology and security experts say. “We are aware these attacks are happening all the time,” said Morgan Eldred, Research Director at American information technology research and advisory Gartner, by phone. Last year, Saudi Arabia’s national oil company Saudi Aramco was hit by a virus that infected as many as 30,000 of its machines. It took nearly two weeks for Saudi Aramco to recover from the damage, disrupting the world’s largest oil producer.

New York financial regulator pushes banks to plug gaps in cyber security (October 27, 2014)
Following the massive cyber attack on the biggest U.S. bank JPMorgan Chase & Co (JPM.N) disclosed in August, and other financial institutions, government authorities in the United States are pushing financial institutions and brokerage houses to close glaring gaps in cyber security.

Computer security threat could be worse than Heartbleed (October 3, 2014)
Internet security experts are warning a new programming flaw known as the “Bash Bug” may pose a serious threat to computers and other devices, such as home Internet routers. Even the systems used to run factory floors and power plants could be affected.

The one cybersecurity threat everyone misses (October 10, 2014)
After a spate of high-profile cyber security breaches at major companies like Target and, more recently, Home Depot and JPMorgan Chase, the biggest players for the most part have strong protections to wall off their proprietary information. But smaller vendors who can't afford expensive security measures—and yet have links to some of their larger client's sensitive data—are now in the crosshairs of sophisticated hackers.

Kmart becomes latest retailer hit by data theft (October 13, 2014)
Sears Holdings Corp. announced late Friday that it detected a data breach at its Kmart stores that started last month and that certain customers' credit and debit card accounts may have been hacked. The data theft at Kmart is the latest in a string of incidents that have hit several big retailers, including Target, Supervalu and Home Depot.

Featured Post: Online Security Experts Link More Breaches to Russian Government

For the second time in four months, researchers at a computer security company are connecting the Russian government to electronic espionage efforts around the world. In a report released on Tuesday by FireEye, a Silicon Valley firm, researchers say hackers working for the Russian government have for seven years been using sophisticated techniques to break into computer networks, including systems run by the government of Georgia, other Eastern European governments and militaries, the North Atlantic Treaty Organization and other European security organizations. Read the article here.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2014 / Issue 37

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.

Schneider Electric

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

1820 Preston Park Blvd. Suite 1900 Plano, TX 75093 ▪ P 469.365.6400 ▪ F 888.758.7675 ▪ **iom.invensys.com**