The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

August 2015
Volume 47

Huge gap in cyber security knowledge leaves Asia vulnerable (APAC)

From thejakartapost.com, 8/24/2015

ESET®, a global pioneer in proactive protection for more than two decades, released the ESET Asia Cyber Savviness Report 2015 which shows that 93 percent of online users in Asia worry about cyber security. The survey also underlines that the region still has a long way to go in understanding online security and protecting themselves. In fact, 3 out of 5 consumers are unable to answer basic cyber security questions correctly. Other findings of the report include:

- Over 38 percent of users across the region engage in risky behavior online, despite knowing the dangers
- 4 in 10 users gain information about cyber security through unofficial sources
- Malaysia takes the lead as the most cyber-savvy nation while Indonesia is on the bottom rung in this regard

this issue

A Tribute to Ernie Rakaczky

This month we are paying a special tribute to a friend and colleague who started beating the drum of cyber security in Industrial Automation. Back in 2001, Ernie Rakaczky started conversations about why companies should secure their plants—something that had been largely overlooked. Ernie was always the voice of reason for why companies should consider cyber security controls at a plant. Year after year, Ernie tirelessly presented this message to the industry and to our executives. He participated in the efforts at ISA within SP99, Automation Federation, NIST -SMART GRID, MSMUG, and within ICSJWG from DHS. He also played an active role in the various security initiatives with DOE, DHS, INL, NRC, NPRA, IAEA, and SANDIA. Ernie was instrumental in making anti-virus software a standard shippable item with the Foxboro system, which was an industry first. He always pushed a positive position for the benefits of cyber security for our company and our clients.

Ernie played an active role within the process control arena for over 30 years with the past 10 years fully dedicated to addressing cyber security requirements for process control systems and raising the overall protection of our global infrastructures. He ensured a clear understanding and focus on cyber security requirements within all product strategies at Invensys. Additionally, Ernie was a founding member of the Canadian Industrial Cyber Security Council and was appointed by Public Safety Canada to chair an active working group to define the Cyber Security Requirements for the Canadian Critical Infrastructure. Ernie also has a patent for cyber security in ICS for "process control methods and apparatus for intrusion detection, protection and network hardening."

Ernie may have lost his two-year battle with cancer, but his message and efforts will continue with the people he inspired. The very basis of our cyber security program and offerings come from Ernie and his push to get it done.

Cyber Security Services by Schneider Electric

August 2015 / Volume 47

Remembering Ernie Rakaczky

We had the immense pleasure of working with Ernie on the early beginnings of the Invensys and McAfee partnership. We will be forever grateful to Ernie for his mentorship, guidance, and friendship. Ernie worked tirelessly to coach and educate McAfee on the unique requirements for the critical infrastructure space. I fondly remember one particular time when we were working with Ernie in a three-day workshop with long hours and business dinners. It was around Christmas time. Ernie was the most unselfish participant of the workshop, always passionate about sharing his knowledge and expertise for the betterment of the team. After three non-stop days of work, we were all rushing to catch our flights home. Ernie asked me if we could go to the closest Toys "R" Us so he could pick up some very specific Christmas gifts for his kids as well as the candy store for some very specific candy that he knew his kids liked. I will always remember this particular event with Ernie because in this seemingly small act of going to Toys "R" Us and the candy store, it was obvious how deeply Ernie loved his family. My memory of Ernie will always be of an extremely passionate and hard-working professional but mostly for the image I have in my mind of Ernie anxious to get to Toys "R" Us and the candy store to get special gifts for his family that he knew they would love. In this moment, I saw a glimpse of Ernie that I will always remember affectionately. Thank you for everything, Ernie.
—Sheila McLaughlin, McAfee

Ernie was a true friend and as we joked often that we were "brothers from different mothers." He was the type of guy you could argue with but always manage to land on common ground before the dust settled. His passion for cyber security in industrial control systems was only exceeded by his love of family. I felt privileged to know both sides of him and will miss him dearly. He is one of those people that will never really be gone as he left such a warm and fruitful legacy behind. Our industry owes him a precipitous debt of gratitude. Wherever there was an initiative that was worth endorsing, you would find Ernie's name as a founder, working on both sides of the border, treating the world as one.
—Paul Forney, Schneider Electric

Ernie's efforts to increase awareness for better cyber security within industrial computing systems are second to none. Not only was he a great cyber security evangelist, he was also a great friend. I miss traveling the world with him. And most of all, a business dinner without Ernie ordering chocolate ice cream will never be the same.
—Clayton Coleman, Schneider Electric

I was first introduced to Ernie at a cyber security conference where he was talking shop and shaking hands and working the room with others in the industry—something Ernie was truly meant to do. Ernie shared with me his vision for cyber security, which ranged from solutions and products to marketing. Ernie was a true cyber security visionary for Invensys. His omnipresence will always be felt.
—Tom Jackson, Schneider Electric

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
August 2015 / Volume 47

Industry News

Military leaders warn U.S. is falling behind in cyber security (NA)

From www.washingtonexaminer.com, 8/27/2015

The United States is at risk of falling behind its enemies in the field of cybersecurity, military leaders said this month. The comments come after an unclassified server of the Pentagon's Joint Chiefs was penetrated this month by a state-affiliated hacker believed to be Russian or Chinese. That incident, Defense Secretary Ash Carter told Defense One, "is evidence that we're not doing as good as we need to do in job one in cyber, which is defending our own networks.

APAC banks unprepared for cyber threats (APAC)

From www.telecomasia.net, 8/1/2015

Despite cyber security being a clear priority, more than half (64%) of Asia Pacific's senior bank executives feel their organizations are unprepared for today's cyber attacks, according to a survey conducted at FICO's Asia Pacific CRO Forum. According to a 2014 PwC report, cyber crime is the second most prevalent economic crime faced by financial institutions and 36% of people in financial services expect to experience cyber crime in 2015. FICO's survey shows that while cyber security has become a top priority for leadership, APAC banks may not be up-to-date on the latest technology. Some 58% of respondents in the FICO survey said they had not heard of a predictive analytics alternative to traditional rules-based SIEMs.

Asean organizations braced for cyber attack (APAC)

From www.computerweekly.com, 8/1/2015

The high-profile data breaches at Sony Pictures, Target and other US-based companies that dominated the news in 2014 have raised awareness of cyber crime. But two years before these headline-grabbing incidents, governments and companies across Southeast Asia had already been contemplating the impact of a borderless digital economy where crimes can easily be committed online. The sub-region has seen an increase of Internet-related crimes even as local law enforcement agencies have started cracking down on cyber criminals based in their countries. With the growing sophistication of cyber threats, companies in Southeast Asia are going beyond the simple antivirus and firewall they used to employ in their organizations.

New Threats To Caribbean Cyber Security (CARIB)

From jamaica-gleaner.com, 8/16/2015

Cybersecurity incidents continue to rise. According to PwC's Global State of Information Security Survey 2015, attacks rose internationally by 48 per cent in 2014, resulting in huge remedial and reputational costs to the companies and governments concerned. Despite this, the Caribbean remains woefully unprepared with governments and parts of the private sector declining to take the matter seriously until subject to an attack. The danger was borne out earlier this year when St Vincent & the Grenadines and The Bahamas saw their government websites taken over by those claiming to support militant groups fighting in the Middle East. These attacks, while seemingly matters of little consequence, were far from it. They revealed not just the lack of appropriate security within government portals, but the existence of outmoded IT systems and software with the potential, some experts suggest, to have compromised government's internal communications. They also demonstrated the potential vulnerability many, if not most Caribbean states, have to a cyber attack on critical infrastructure.

Department of Homeland Security reveals top sector at risk for cyber attacks (NA)

From www.ibamag.com, 8/14/2015

The increasing importance of cyber risk insurance has been well-documented, but new information suggests one industry is more at risk of cyber attacks than any other. According to data from the Department of Homeland Security (DHS), more than 50% of investigated cyber incidents from October 2012 to May 2013 occurred within the energy sector. Specifically at risk are power and utilities companies, which provide heat and electricity to homes and businesses across the US.

Cyber attacks threaten natural gas industry (NA)

From www.washingtonexamier.com, 8/24/2015

The administration is seeing a "big and growing threat" from possible cyber attack against the nation's natural gas infrastructure, as well as new cars and the sprawling traffic management system. Energy Secretary Ernest Moniz said the utility sector is usually the "poster child" for the threat the U.S. faces from cyber attacks, but there is also a threat to natural gas compressor stations, vehicle traffic management system, and new cars and trucks that have much more digital hardware that makes them increasingly vulnerable to being hacked. He said much more has to be done on training cybersecurity specialists to counter the threat, but "training of professionals [is] ... not keeping up with demand."

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
August 2015 / Volume 47

Cyber News

Hacking-enabled insider trading underlines need for cyber legislation

From www.computerweekly.com, 8/7/2015

The number of people charged in connection with insider trading based on information stolen by hackers has increased to 32, underlining the need for legislation to strengthen cyber security. Initial reports indicated that only nine suspects were to be charged by US authorities in Brooklyn, New York and New Jersey in connection with insider trading based on stolen corporate press releases before they had been made public. The insider trading gang is estimated to have netted more than $100m in illegal profits from 1,000 alleged insider trades over three years, up from initial estimates of $30m, reports the BBC. The hackers – believed to be based in Ukraine and possibly Russia – broke into the computer systems of PRNewswire Association, Marketwired and Business Wire.

Tesla looking to recruit hackers to strengthen its cars against cyber attacks

From au.idigitaltimes.com, 8/11/2015

During the annual Def Con event this month in Las Vegas, carmaker Tesla recruited hackers in the event in an effort to protect its vehicles from possible cyber attacks. This news comes after the exposure of how vulnerable to hacking automobiles from Fiat Chrysler and GM are, and its lack of cyber security knowhow. “Hackers are a crowd that is really important to us,” Tesla communication manager Khobi Brooklyn said. “It is a community that we want to be a part of, and collaborates with, as well as recruit from.”

IRS says cyber attacks more extensive than previously thought

From www.reuters.com, 8/17/2015

The U.S. Internal Revenue Service (IRS) said a hacking attack into one of its computer databases revealed in May was much more extensive than previously thought, with nearly three times as many taxpayers hit by data theft. The IRS said in late May the tax return information of about 114,000 U.S. taxpayers had been illegally accessed by cyber criminals over the preceding four months, with another 111,000 unsuccessful attempts made. A new review has identified 220,000 additional incidents where data was breached, the tax collection agency said. It identified another 170,000 suspected failed attempts by third parties to gain access to taxpayer data.

Security firm uncovers cyber attack campaign against India and neighboring countries

From www.dnaindia.com, 8/24/2015

Cyber Security firm FireEye has published a report revealing that India has been the victim of an advanced campaign of cyber attacks over the past few years. According to the report, the campaign appears to target information about ongoing border disputes and other diplomatic matters in India, Bangladesh, Nepal and Pakistan. The group behind the operation, which FireEye believes is most likely based in China, sent targeted spear phishing emails containing Microsoft Word attachments to its intended victims. These documents pertained to regional issues and contained a script called Watermain, which creates backdoors on infected machines. The campaign’s attacks were also detected in April 2015, about one month ahead of Indian Prime Minister Narendra Modi’s first state visit to China.

Healthcare institutions at risk of cyber attacks

From www.buildings.com, 8/26/2015

Due to the high-value nature of their information, healthcare institutions are a common target for hackers – a new survey shows that 81% of healthcare executives report that their organizational infrastructure has been attacked or compromised by one or more malware, botnet, or cyberattacks during the past two years. The 2015 KPMG Healthcare Cybersecurity Survey, which polled 223 executives at U.S. healthcare providers and health plans, also showed that only half feel they are adequately prepared to prevent attacks and 16% can’t detect a breach in real-time. Additionally, the researchers also found that attacks are on the rise, with 13% of respondents saying their organizations are targeted about once per day and another 12% reporting two or more attacks per week. The report notes that in terms of revenue, larger organizations are better prepared to defend against cyber threats than smaller ones. According to the survey, the most vulnerable areas include external attackers, sharing data with third parties, employee breaches, wireless computing, and inadequate firewalls.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
August 2015 / Volume 47

Keeping Things Secure on the Road

As cyber security becomes a larger part of the daily lives of organizations, many of them have started implementing countermeasures at their corporate office locations, such as enterprise detection and monitoring tools, robust logging systems, intrusion prevention and detection systems, and other systems that will protect their users from the outside world when connecting to the internet from the office. However, when the internet provider is not a trusted entity, and when a user is connecting through untrustworthy network connections, such as a hotel or airport wireless system, these protections can be nullified by an attacker in the middle monitoring and tampering with the data before it reaches its destination.

One major source of these man-in-the-middle attacks is someone setting up a device to spoof a public Wi-Fi hotspot or router, and once a user connects to their fake device, intercepting traffic and getting important data, such as business data, banking data, or other sensitive information. These types of attacks are particularly common in public areas, such as coffee shops, airports, hotels, or other areas where people expect free public Wi-Fi. Having corporate assets such as laptops or tablets “in the wild” can lead to users to inadvertently subject themselves to these types of attacks and give up corporate data, all without realizing anything has occurred.

The primary defense against these types of attacks are using encryption and authentication between your endpoint devices and whatever they are communicating with to ensure no third party is snooping on the traffic or changing it mid-stream. If strong encryption is used, it would be nearly impossible for an attacker to have the ability to un-encrypt it, modify it, and re-encrypt it in real-time. To ensure this is occurring, employees should always connect to websites that use Secure Sockets Layer connection by only navigating between websites that use HTTPS connections. However, there are ways around this with SSL strippers that can negate this security. To truly control this security, organizations should look into using VPN solutions that the employee must use when connecting their assets outside of the corporate locations. Using a VPN will authenticate the user and encrypt all of the traffic that the user generates, preventing a man-in-the-middle attack. In addition, this will allow the user to connect back to the corporate network and gain the extra benefits from being protected by all of the central cyber security solutions deployed there.

Cyber security is important in this changing landscape, but all locations where data is accessed must be considered in order to create a full and robust cyber security program. Because of this, ensuring that your organization has a plan for defense when employees have corporate assets outside of the office is necessary to fully protect critical data.

This month’s contributor to Consultant’s Corner is Gary Kneeland
Consultant, Cyber Security Services
gary.kneeland@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
August 2015 / Volume 47

Cyber Security Services

Schneider Electric's Cyber Security Services organization has the 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 Cyber Security Services include:

Hardware Independence

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

Regulation Knowledge

Cyber Security Services 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 Cyber Security Services 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 WordPress!

Industry Knowledge

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

Proven Methodology

Cyber Security Services follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the lifecycle approach are Assessments, Development, Implementation, and Management.

Schneider Electric

For additional information please visit us at
http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/

1650 West Crosby Road, Carrollton, TX 75006 ▪ P 972.323.1111 ▪ F 888.758.7675 ▪ www.schneider-electric.com