The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

August 2014
Issue 35

More than 1,000 businesses hit by same cyber attack as Target

From mashable.com, 8/22/2014

Target wasn't the only business that experienced a cyber attack that compromised tens of millions of its customers' credit cards, according to the Secret Service. More than 1,000 American businesses were hit by the same cyber attack that affected in-store cash registers at Target last year, The New York Times reported. According to a Department of Homeland Security advisory obtained by the New York Times, the attacks were "much more pervasive" than initially reported as hackers received access to millions of payment card data being sold on the black market. Homeland Security officials encouraged all businesses, "regardless of size," to check for "Point of Sale malware infections," according to the report.

Invensys is becoming Schneider Electric

this issue

Need for Global Compliance Grows

It has been proven time and again that cyber security knows no border, business, or industry. With the press surrounding the NIST framework as a versatile tool for cyber security compliance, virtually every country is taking some kind of cyber security initiative. Just in this past month, Germany proposed a tougher cyber security law that "requires companies in critical sectors to register any hacker attack" (www.dw.de). These areas include industries like energy, water, and information technology. Singapore has even announced that it is working to bolster its cyber security measures to prevent attacks on its government websites in addition to upgrading its Cyber-Watch Centre, which will help officials track when attacks occur and mitigate cyber threats.

Even the UAE, which was recently identified as being vulnerable to cyber attacks due to its growing defense sector, continues to push for meeting compliance requirements (thenational.ae). And the EU-funded CIPHER project seeks to prevent cybercrime by introducing a cyber security framework for information systems (cordis.europa.eu).

There has been a global increase in the number of organizations and entities that are focusing on cyber security compliance that specifically address critical infrastructure:

- Europe has the European Program for Critical Infrastructure Protection (EPCIP)
- UK has the Centre for the Protection of the National Infrastructure (CNPI)
- Latin America has its own comprehensive cyber security strategy that was adopted by OAS
- Asia-Pac countries are addressing cyber security through organizations such as the International Multi-Lateral Partnership of Cyber Threats (IMPACT) and National Information Security Center (NISC)

No matter what business or industry, any company's cyber security program must begin with cyber security compliance, whether these compliance requirements are federal, state, or corporate directives.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2014 / Issue 35

Industry News

UAE records highest computer breaches across the Middle East

From www.khaleejtimes.com, 8/6/2014

As more high-level threats to cyber security in the region emerge, data shows the UAE has the highest number of computer system breaches across the Middle East. Computer software company Symantec recently said a three -year investigation showed a new attack group—dubbed 'Dragonfly'—conducted a prolonged and sophisticated cyber espionage campaign against the global oil and gas sector, likely emanating from a professional Eastern European state-sponsored group. There are more than 1,000 active infections in 84 countries. Symantec data showed the UAE has consistently had the highest number of ongoing infection detections in the Middle East on a monthly basis since last July, peaking at 500,000 at the end of last year.

Power sector is just as vulnerable to cyber attacks

From vpncreative.net, 8/7/2014

While there is hardly any industry that has escaped the notorious attempts of hackers, critical industries such as energy face a higher risk of cyber attacks, according to a recent study from Unisys. The survey, spanning 13 countries and 599 info-tech executives, was recently conducted by Ponemon Institute to decipher the readiness of companies working in the utility, manufacturing, and energy sectors against probable cyber attacks. The Unisys-sponsored survey revealed that most of these companies have hardly any infrastructure in place to fight such attacks. Cyber experts in the US have started giving more attention to the power and oil industry that is highly susceptible to such attacks. The growing concerns aren't without proof. According to an agency report, out of the 200 infiltration attempts handled by the Department of Homeland Security, more than 40 percent were aimed at the industries related to the energy sector.

Skills gap leaves UK vulnerable to cyber attack, says business

From technologyinsider.co.uk, 8/6/2014

Business chiefs have warned that a skills gap is leaving the UK vulnerable to cyber attack, as statistics show that fewer than 0.6 per cent of recent graduates are working in cyber security. The quality of computer science degree programs is being blamed, with industry leaders stating that graduates are ill-equipped for the modern workplace as they have studied little in the area of cyber security, which constitutes less than 5 per cent of degree credits in some institutions. An analysis of higher education students in 2012-13 conducted by the International Information Systems Security Certification Consortium, an industry body, showed the number of computing science first degree graduates in employment was 7,635, of which just 0.6 per cent were in cyber security roles.

Iran attempted large-scale cyber-attack on Israel, senior security source says

From www.jpost.com, 8/17/2014

Iran attempted to conduct a large-scale cyber-attack on Israeli civilian communications during the war with Hamas this summer, a senior security source revealed. "This is not something we have seen before, both in terms of scope and the type of targets. They targeted communications infrastructure that belong to the civilian sector in Israel," the source said. Iranian elements were definitely behind the attack, he said, though their aim to cause maximum disruption, was not achieved. Cyber attackers targeted IDF websites, but online defenses withstood the assault, the source said.

U.S. government's nuclear watchdog victim of cyber attacks

From www.reuters.com, 8/19/2014

The U.S. Nuclear Regulatory Commission was "successfully hacked" three times in recent years in attacks involving tainted emails, according to an internal investigation on cyber attacks at the agency, Nextgov.com reported. At least two of the attacks originated overseas, according to the report obtained by Nextgov, a rare public report with details of a cyber attack on the energy sector. The publication said it obtained a copy of a report by the NRC's Office of the Inspector General, which reviewed 17 suspected breaches from 2010 to 2013.

Japan must beef up measures to protect nation from cyber attacks

From www.chicagotribune.com, 8/25/2014

According to an annual report the government released last month, there were 5.08 million cases of illegal access to government organizations' computer networks in fiscal 2013. This figure is five times the level in the previous fiscal year. A majority of the cases are considered to be cyber attacks aimed at stealing important government information. Many are believed to have come from abroad, from places such as China. During the period from August to September last year, many advanced persistent threat (APT) attacks were made on central government bodies including the ministries of finance; foreign affairs; economy, trade and industry; and the agriculture, forestry and fisheries.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2014 / Issue 35

Cyber News

Thai cyber security slammed

From www.bangkokpost.com, 8/2/2014

A report conducted last year by England's Sophos found Indonesia, China, Thailand, the Philippines, Malaysia, India, Mexico, the UAE, Taiwan and Hong Kong were the 10 riskiest places. Thailand is also the world's second-most vulnerable location to access bank ATMs, said the European ATM Security Team. Nearly 100 Thai government websites have been hacked and used to distribute malware, representing 85% of all government-hosted malware in the world, said a report by English internet services firm Netcraft Ltd.

Russian cyber attack 'could cost £1.4bn'

From www.telegraph.co.uk, 8/7/2014

A cyber attack by a Russian hacker group that resulted in the theft of 1.2 billion internet credentials from major companies around the world could cost £1.4 billion, according to an insurance group. The attack, which came to light on Tuesday, allowed hackers to steal confidential user names and passwords from some 420,000 websites, ranging from household names to small Internet sites. Hold Security, which uncovered that attack, did not give details of the companies affected. However, it described it as the "largest data breach known to date."

Latin America cyber security market is expected to reach $11 billion in 2019

From insurancenewsnet.com, 8/10/2014

The Latin America Cyber Security report defines and segments the cyber security solutions and services market in Latin America with analysis and forecast of revenue. This market is estimated to grow from around $5.29 billion in 2014 to $11.91 billion by 2019, at a CAGR of 17.6% from 2014 to 2019.

Community Health says data stolen in cyber attack from China

From www.reuters.com, 8/18/2014

Community Health Systems Inc (CYH.N), one of the biggest U.S. hospital groups, said on Monday it was the victim of a cyber attack from China, resulting in the theft of Social Security numbers and other personal data belonging to 4.5 million patients. Security experts said the hacking group, known as "APT 18," may have links to the Chinese government. "APT 18" typically targets companies in the aerospace and defense, construction and engineering, technology, financial services and healthcare industry, said Charles Carmakal, managing director with FireEye Inc's (FEYE.O) Mandiant forensics unit, which led the investigation of the attack on Community Health in April and June.

Cyber security threats rise in frequency, complexity

From www.eweek.com, 8/13/2014

Cyber-threats, data breaches and high-risk vulnerabilities have continued to dominate the first half of 2014, with attacks affecting consumer's personal information, included theft of data such as customer names, passwords, email addresses, home addresses, phone numbers, and dates of birth, according to a report from Trend Micro. The data breaches and Distributed Denial of Service (DDoS) attacks recorded this quarter showed that an organization-wide strategy is required if companies wish to survive their aftermath. Organization-wide, understanding and commitment to carrying out a strategic security plan is necessary. Otherwise, they may resort to highly impractical measures such as reverting to manual processing, as in the case of P.F. Chang's restaurant, the report noted.

UPS stores hit by cyber attack, customer data compromised

From finance.yahoo.com, 8/22/2014

Leading freight forwarding company, United Parcel Service, Inc. (UPS) is the latest to fall prey to cyber attacks. The company has reportedly faced malware attacks across 51 U.S. stores, which represents 1% of the existing 4,470 UPS stores in the U.S. According to the company, customer details such as debit and credit card information for cards used in any of the breached stores may likely be exposed to hackers who have caused these cyber crimes in the UPS system.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2014 / Issue 35

The Need for Cyber Security Awareness

In today's environment, where nearly everyone utilizes personal computing devices—from desktop computers to smart devices—and security failures are becoming daily occurrences, it is imperative to raise the user's cyber security awareness and adherence to security policies and procedures.

In many industries, there are many satellite locations that sit outside the focus of the corporate center. Many of these locations are understaffed, and employees feel that cyber security is an additional burden that they do not have time for. These locations present easy targets for today's skilled hacker. Firewalls and other security controls provide baseline protection; however, they can be rendered useless if a user misuses their access or fails to protect resources, such as user IDs or passwords.

To raise awareness, companies should provide regular training that is consistent company-wide and reinforces the security policies and procedures that are in place. This training should not focus on the details of regulations, but rather focus on the general requirements and good practices users should take away and make part of their daily routine.

Cyber security awareness provides a foundation for addressing the fundamental principles of cyber security—protecting the confidentiality of information, ensuring the integrity of information, and ensuring the availability of information and resources. By raising cyber security awareness, a company can minimize the cost of security incidents and assure the consistent implementation of security controls throughout the organization.

This month's contributor to Consultant's Corner is Michael Gasparovic
Consultant, Critical Infrastructure & Security Practice, Invensys
michael.gasparovic@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2014 / Issue 35

Most Popular Blog Posts This Month

Home Security Systems Can Be Hacked (July 31, 2014)
Dale Baker has an ADT home security system. He'd be at home when it would start chirping. "I was hearing that a lot, but no doors or windows were open," Baker says. He called the company and learned something that disturbed him. His system is wireless and signals from the sensors on doors and windows could be intercepted.

Warning Over Android Security Risk (August 1, 2014)
A new flaw in the Android mobile operating system leaves the personal and financial details of users since 2010 at risk to hacking, a mobile analytics firm has claimed.

Researcher says PayPal's two-factor authentication is easily beaten (August 6, 2014)
A security feature offered by PayPal to help prevent accounts from being taken over by hackers can be easily circumvented, an Australian security researcher has found.

U.S. Homeland Security contractor reports computer breach (August 8, 2014)
A company that performs background checks for the U.S. Department of Homeland Security said on Wednesday it was the victim of a cyber attack, adding in a statement that "it has all the markings of a state-sponsored attack." The computer breach at Falls Church, Virginia-based US Investigations Services (USIS) probably involved the theft of personal information about DHS employees, according to the Washington Post, which first reported the story.

AT&T hackers in PHL arrested (August 15, 2014)
Six people were arrested by the anti-cybercrime police for allegedly hacking the system of American telecommunication company AT&T, causing about $24 million loss from the company, police said Thursday.

Featured Post: 8 ways to bullet proof your social accounts

There are ways to keep the hackers at bay-for the most part, anyways, since no protection is 100 percent efficient. Click here to read about tips to protect yourself from attacks.

Visit us on Blogger!

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
August 2014 / Issue 35

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**