January 2012 / Issue 04

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

- 2012: What lies ahead?
- Hacktivism
- Industry News
- Invensys CISP News

2012: What lies ahead?

NERC-CIP 2011

Total Fines
2011 YTD
$7.73MM
Total
$16,02MM

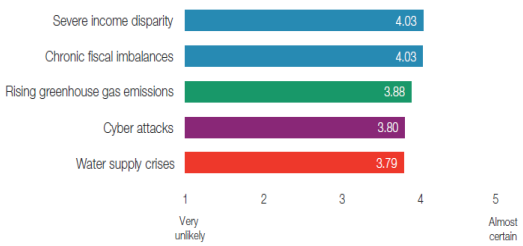
Avg. Qrtly. Fines Up
4Q was $220K
1Q-3Q was $72K

Violations
All Violations
132
CIP Violations
81

CIP to non-CIP
Violations Up
2011 YTD >61%

2011 was a very interesting year for Cyber Security. There was much follow-up on Stuxnet. The rise of national cyber attacks, originating from within China. Verified attacks on a water utility in Houston, TX and a nuclear facility in France. 2011 ushered in a new phrase in our lexicon—Hacktivism, the act of hacking, or breaking into a computer system for a politically or socially motivated purpose.

What lies ahead for 2012? Unfortunately, more of the same. The World Economic Forum, an organization that typically focuses on geopolitical unrest, global economic forecast, and academic research listed Cyber Security at #4 in the recent Global Risk 2012 report. The ranking is based on a 10 year outlook and their survey captures the perceived impact, likelihood, and interconnectedness of 50 prevalent global risks. The top 5 have the highest perceived likelihood and potential impact and are listed below.



Threats from Cyber Attacks have been thrust into the limelight due to the events of the past few years. Gone are the notions that a company or industry is too small, too well-protected, or just not "the type of company someone hacks." As indicated by the World Economic Forum and others, it is now an issue of "When" vs. "If" for cyber attacks.

A few other 2012 trends to watch:

Securing The Human
Humans are the weakest link, regardless of how technology changes. Weak passwords, thumb drives, and poor access control will always be the Hacker's preference.

Security trumps compliance
Security decisions have typically been driven by compliance due to the influx of new regulations driving the budget. Now, with the cost of security breaches rising along with the increasing probability of a cyber security incident, companies are realizing the need to protect their intellectual property and critical assets and will begin to make cyber security decisions based on security.

Increased Regulatory Scrutiny
In addition to regulations such as NERC CIP, NEI, CFATS, and others, the US government has made Cyber Security a priority for the future.

Hacktivism

US government hits Megaupload with mega piracy indictment (SOPA)

From Gizmodo.com 1/18/2012

Seven executives charged as filesharing site shut down over accusations that they cheated copyright holders out of $500m.

Operation Blackout

From Anoncentral.org 1/19/2012

This is an urgent emergency alert to all people of the United States. The day we've all been waiting for has unfortunately arrived. The United States is censoring the internet. Our blatant response is that we will not sit while our rights are taken away by the government we trusted them to preserve. This is not a call to arms, but a call to recognition and action!

-We are Anonymous.
-We are Legion.
-We do not forgive censorship.
-We do not forget the denial of our free rights as human beings.

To the United States government, you should've expected us.

Anonymous goes on Megaupload Revenge spree: DoJ, RIAA, MPAA, and Universal Music all offline

From Gizmodo.com 1/20/2012

Anonymous has sure been quiet lately, but today's federal bust of Megaupload riled 'em up good: a retaliatory strike against DoJ.gov (and plenty of other foes) leaving them completely dead.

Internet wins: SOPA and PIPA both shelved

From Arstechnia.com 1/20/2012

Just hours after Senator Harry Reid (D-NV) announced he was delaying a vote on the PROTECT IP Act, Rep. Lamar Smith (R-TX), the sponsor of the Stop Online Piracy Act, followed suit and announced he would be delaying consideration of the companion legislation. "I have heard from the critics and I take seriously their concerns regarding proposed legislation to address the problem of online piracy," Smith said. "It is clear that we need to revisit the approach on how best to address the problem of foreign thieves that steal and sell American inventions and products."

Intelligence firm Stratfor reels after data breach. What did hackers get?

From CSMonitor.com 12/26/2011

Stratfor, the private firm based in Austin, Texas, provides analysis of geopolitical and security issues to clients who range from the US military to large corporations.

Hackers breached the firm's computer systems, claiming to act as the group known as Anonymous, which has perpetrated other cyber attacks this year. The online infiltrators released thousands of credit card details, passwords, and home addresses from Stratfor's private client list via the information sharing website Pastebin.

Anonymous shreds intelligence firm Stratfor in latest hack

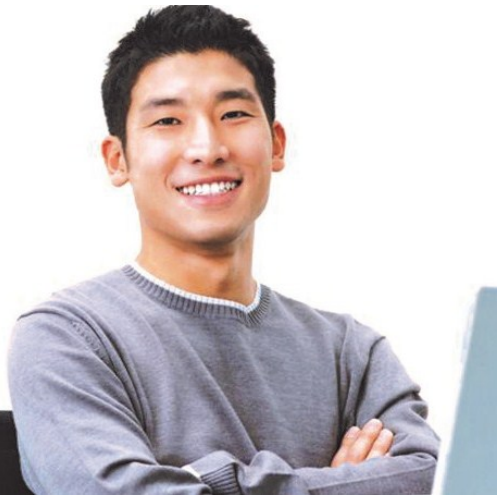
From SCMagazine.com 1/06/2012

In what may be its most devastating attack since HBGary, the Anonymous hacktivist collective rooted the database of security intelligence firm Stratfor to plunder a claimed 200 gigabytes of data. As of Sunday afternoon, Stratfor's website was offline for maintenance, and Anonymous was posting to Pastebin samples of its booty, including Stratfor's extensive client list—which consists of many major companies and law enforcement agencies—and stolen credit card information belonging to members.

Hackers hit Stratfor again, but this time just for laughs

From MSNBC.com 1/06/2012

Subscribers were asked to rate the company's handling of the attack, but it's really AntiSec again. The hackers behind the year-end attack on the security consulting firm Stratfor have struck again, although this time it appears they are just out for a few laughs.



Industry News

Over 10,000 ICSes found connected to public internet due to poor security practices

From Wired.com 1/24/2012

A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices. Infrastructure software vendors and critical infrastructure owners have long maintained that industrial control systems (ICSes) —even if rife with security vulnerabilities—are not at risk of penetration by outsiders because they're "air-gapped" from the internet; that is, they're not online.

Cyber threat to power grid puts utility investors at risk

From Forbes.com 12/27/2011

The electric utility industry's concerns about cyber security have escalated sufficiently for several investor-owned utilities to include cyber attacks as a material risk factor. Recent filings with the U.S. SEC. Consolidated Edison of New York included cyber attacks as a risk factor that could affect investors' quarterly report (10-Q) for the first time. Pepco Holdings, a large power and gas utility includes cyber attacks in a broader, catch-all disclosure about terrorism and other mega-catastrophes.

The cost of hackers

From The Wall Street Journal

Kuwait billionaire Bassam Alghanim was recently the victim of a cyber attack when his brother, Kutayba, paid Chinese hackers a mere $400 to illegally access his email so that he could publish personal information online, which included nearly two years' worth of emails containing information about "personal finances, legal affairs, and even pharmacy bills." Websites like hire-to-hack.com offer easy and accessible ways to hire hackers who can "crack passwords for major email services in less than 48 hours," and some sites even offer short tutorials and tips for hacking.

Cyber attacks could wreck world oil supply

From The Wall Street Journal 12/2011

Hackers are bombarding the world's computer-controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil supply disruption. Oil company executives warned that attacks were becoming more frequent and more carefully planned. "If anybody gets into the area where you can control the opening and closing of valves or release valves, you can imagine what happens," said Ludolf Luehmann, an IT manager at Shell Europe's biggest company. "It will cost lives and it will cost production, it will cost money, cause fires and cause loss of containment, environmental damage—huge, huge damage," he told the World Petroleum Congress in Doha.

Mac malware becomes more serious

From infoworld.com 1/19/2012

Although most hackers target computers with Windows operating systems, recent reports show that Macs have recently been targeted with malware that has lasting impacts. The Mac malware threat has become much more serious since a series of "rogue security programs released under various names, including Mac Defender and MacGuard, likely infected thousands of Mac users after its release in early May 2011."

Attacks on utilities, embedded systems, and mobile devices seen rising in year ahead

From infoworld.com 1/2012

Some of the more intriguing security issues for 2012 are "going to be around industrial attacks, hacktivism, and embedded threats," Marcus said. "That's where some real dangers lie—when you talk about knocking a utility company offline, that's a big deal."

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
January 2012 / Issue 04

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 Consulting include:

Hardware Independence

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

Industry Knowledge

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

Regulation Knowledge

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

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, Implementation, and Management.

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.

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**