2017 Cyber Risks to Intensify as Hackers Become More Cunning: Report

Posted on January 11, 2017

(http://www.energi.com/news/2017/01/2017-cyber-risks-to-intensify-as-hackers-become-more-cunning-report/)

Click here (http://www.insurancejournal.com/news/international/2017/01/11/438549.htm) for the source.

Top cyber threats during 2017 are expected to include nation state cyber espionage, a rise in data integrity attacks and an increase in attacks harnessing Internet of Things (IoT) devices, according to a report published by Stroz Friedberg, an Aon company.

Cyber attacks will intensify this year as "exploit techniques become more cunning," said the report, titled "2017 Cybersecurity Predictions (https://www.strozfriedberg.com/wp-content/uploads/2017/01/2017-Stroz-Friedberg-Cybersecurity-Predictions-Report.pdf?__hssc=151509478.3.1484130512082&__hstc=151509478.32f3d2010971d8f6f96616cb4b689a52.1484130512081.1484130512081.1484130512081.1&hsCtaTracking=d55e3826-9853-4c20-a525-aa8dd662b642%7Cbd412063-f249-44de-800f-1583fd96dbd9)."

"In 2016 we witnessed everything from cyber attacks influencing public opinion to hacked IoT devices and the introduction of new cyber security regulations," said Ed Stroz, co-president and co-founder of Stroz Friedberg, in a statement accompanying the report.

"This year we'll see an intensification of these threats, along with new challenges and a blurring of lines between the actions and responsibilities of the state, markets, businesses and civil society," he added.

"The flood of fake news and nation state-backed attacks in this past year's election are just a sign of things to come, as attackers find new ways to seek faster and wider access to data and exploit sensitive information," he warned.

As governments respond to the threats posed by cyber risks by firming up their online regulatory regimes, businesses may find themselves burdened by the need to interpret "a fragmented global regulatory landscape" and what that means for their operations, the report indicated.

There will be a "necessity to accept that cyber security risk management is a critical part of doing business," the report continued.

The Stroz Friedberg report lists its top cyber predictions during 2017 (which *Insurance Journal* has presented in a different order):

- **Criminals to harness IoT devices as botnets to attack infrastructure.** There will be an increase in compromised IoT devices, harnessed as botnets and used as launching points for malware propagation, SPAM, distributed denial of service (DDoS) attacks and anonymizing malicious activities.
- **Industry first-movers will embrace pre-M&A cyber security due diligence.** The financial services industry and other regulated sectors will be early adopters of cyber security due diligence as a critical part of the pre-M&A due diligence process, learning from high profile transactions that were derailed in 2016, following the exposure of cyber vulnerabilities.
- **Data integrity attacks to rise.** Data sabotage as the next big threat will become a reality in 2017. "Criminals will seek to sow confusion and doubt over the accuracy and reliability of information, impairing decision-making across the private and public sector," the report added.
- **Spear-phishing and social engineering tactics to become craftier, more targeted and more advanced.** Criminals will increase their focus on the human element as an entry point, exploiting the weakest link – employees – that organizations always find challenging to safeguard. (Such tactics fall into the category of "social engineering").
- **Regulatory pressures will make "red teaming" the global gold standard with cyber security talent development recognized as a key challenge.** Increased pressure from regulators worldwide will push in-house "red teaming" capabilities to accelerate in 2017. [**Editor's Note:** So-called red teaming, or ethical hacking, is designed to detect network, system and security vulnerabilities by taking a hacker-like approach to system, network or data access].

The report also noted that companies, which are not in the cyber business, will face a different challenge: recruiting, motivating and retaining highly technical cyber talent to keep their red teams at the forefront of cyber security. This push will likely first occur in financial hubs such as Hong Kong, Singapore, the EU, and even the U.S.

- **Nation state cyber espionage and information war to influence global and political policy.** Cyber espionage will continue to influence global politics and remains a concern during upcoming elections in Latin America and Europe. "Russia, China, Iran, and North Korea will remain regions of great concern in 2017, as they continue to develop deep pools of cyber-crime talent," the report said.

"As government, business, and consumers balance rapid innovation in technology with changing cyber threats, every year sees an intensification of existing risks, and a number of new emerging ones; 2017 will be no different in that respect," the report confirmed.

What differs this year is the impetus and mandate to act, because governments worldwide, including the Trump administration, will begin to firm up online regulation and policies "simply due to their fear of nation state-style attacks," Stroz Friedberg said.

"With this, businesses in 2017 will be burdened by the need to interpret what a fragmented global regulatory landscape means for its operations," the report said, noting however that the industry is not powerless or relegated to sit by and wait for government directives to manage these risks.

As a result, Stroz Friedberg recommends steps that business leaders can take to shore up operations and boost cyber defenses:

- Optimize company's cyber security posture. Continually assess and prioritize cyber threats and vulnerabilities, and improve incident response (IR) readiness.
- Evaluate insider risk. Ensure your formal program is current.
- Conduct M&A pre-deal cyber due diligence early. Perform alongside compliance and financial due diligence. Assess, protect and leverage intellectual property, and commercially valuable information.
- Consider self-regulation by adopting higher security standards in products and services prior to going to market, even if cost is prohibitive.

Photo: http://www.insurancejournal.com/news/international/2017/01/11/438549.htm

10 Centennial Drive, West Entrance, Peabody MA 01960 1.888.ENERGI.1 helpdesk@energi.com | Developed by GraVoc Associates (http://www.gravoc.com)