what we heard

cybersecurity dinner 2015

Discussion Highlights

In February 2015, President Obama, speaking at a White House Summit on cybersecurity and consumer protection, declared that the Internet has become a sort of Wild West, where private corporations are prime targets of hackers and cyber criminals. Egon Zehnder recently hosted a cybersecurity dinner in Dallas for cross-industry executives in the DFW Metroplex to discuss the challenges of preparing and responding to cyber threats in an increasingly dangerous environment. Egon Zehnder invited executives who would act as first responders in the event of an attack: general counsels, chief information security officers, heads of corporate communications and chief information officers.

The conversation was led by panelists David Chamberlin, Executive Vice President and General Manager at Edelman; Erin Nealy Cox, Executive Managing Director at Stroz Friedberg; and Matt Haltom, Senior Vice President, General Counsel and Secretary at Sally Beauty and was moderated by Kal Bittianda, Selena LaCroix, Kristi Maynor and Chris Patrick, all representing Egon Zehnder.

Here is what we heard:

If you want peace, prepare for war

Sixty-five percent of hacked companies are informed by law enforcement or third parties when they have been breached. In other words, internal sensors are not detecting intruders in the network. Companies need to take a proactive stance by investing in more sophisticated security monitoring functions that are designed to perceive not only unauthorized entry but also exits and lateral movements. Companies should regularly pay auditors to access their systems to monitor for dormant malware (hackers can be extremely patient) or malignant software that has not yet been detected. Asked for their opinion on the most worthwhile type of InfoSec investment, all three panelists suggested regular internal exercises simulating a hack/breach. Companies should hire a “white -hat hacker” to test systems and bubble up vulnerabilities.

Information security as a differentiator

Companies like, Bank of America, IBM and Visa are making Information security (InfoSec) a business differentiator compared with their competitors. For example, they have hired communications directors who are solely responsible for dealing with InfoSec. It greatly improves organizational agility and response when there is a team member, like a head of InfoSec communications or a chief information security officer (CISO), whose sole focus is cyber protection.

Lessons learned in a crisis

Continual monitoring: Hackers can do a lot of damage in 48 hours. Even with software monitoring systems in place, an attack that commences on a Friday evening while no one is physically present to oversee the systems over the weekend can be disastrous.

First steps following a breach: Hire a forensics team that is retained by the company and has the company's best interests in mind. Notify your insurance company. Do not notify government agencies until you are sure that consumer data have been lost (until that time, the law does not mandate notification).

Cooperation with law enforcement: Cooperation and information sharing with the government are important. However, government investigators primarily will be concerned with attribution; that is, who is behind the attack? The priority of a company will be to close the doors and stop the leak of information. Law enforcement will want to publicize progress on an investigation. On the other hand, the victim of the hack will want to be more prudent with external communications in order to maintain consumer confidence.

Disclosure: Do not rush to report the size and scope of the hack. If you are imprecise with those numbers, which is likely in the immediate aftermath, you will have to backtrack. It's better to complete a thorough private investigation before disclosing the breach to partners and customers. Customers will want you to provide them with accurate and confirmed answers to their questions, not speculation before facts have been established.

Economic espionage across industries

Seven years ago, companies primarily concerned with cybersecurity were in finance, retail, pharma and defense. Now all industries are at risk. For example, in the consumer space, product formulas are bought and sold on the black market. Why would a company spend years coming up with a competing formula when it can be bought and paid for via the Internet? Even in the technology space, hackers can access the internal networks of software companies and embed malware in the code gene used to develop consumer products. In essence, software releases can be infected even before going to market, giving cyber criminals access to information on thousands of consumers.

Cybersecurity is an issue that cannot be ignored and one that ALL companies need to consider very carefully in order to survive in an increasingly interconnected and digitally dependent global marketplace.

Market observations of trends and the rise of the CISO

Companies are actively looking for cybersecurity solutions to reduce their exposure, address regulator concerns and protect their customers, employees and profits.

1. Increased interest and investment in new companies and innovative solutions are on the rise.
2. Corporations are making process and policy adjustments (e.g., BYOD policies).
3. The CISO role is being formalized, elevated and/or expanded in companies.

Companies at the forefront of dealing with cybersecurity issues are primarily in five areas: financial services, technology, defense, energy and infrastructure. The threat, however, now extends across all industries.

Company boards are increasingly looking for information security experts to either join the board or serve in an advisory capacity to set a workable and effective information security road map and hire and develop effective IT and InfoSec teams.

Public-private partnerships (exchanges, Business Executives for National Security, presidential working groups, etc.) for collaborating and sharing information to combat cyber crime are expanding to more companies.

The CISO role was first formalized as a result of the Patriot Act in 2001; the 2008 financial crisis then triggered the next wave of hires; and now a third wave is under way, triggered by recent high-profile hacking events at global retailers, banks and other organizations.

A talent pool is emerging. While there is much attention to this topic worldwide, there are emerging pools of U.S. talent from government/military agencies (FBI, NSA, Cyber Command, etc.), large defense contractors/consultancies and established white-hat organizations.

The Egon Zehnder Team

Kal Bittianda
New York
kal.bittianda@egonzehnder.com
+1 212 519 6070

Kal Bittianda is a consultant in the New York office of Egon Zehnder and a core team member of the Technology, Telecommunications and Financial Technology Practices focused on emerging technologies, information technology and cybersecurity.

Selena LaCroix
Dallas
selena.lacroix@egonzehnder.com
+1 972 728 5975

Selena LaCroix, based in Dallas, is the Global Leader of Egon Zehnder's Legal Practice Group and Semiconductor Practice Group. Selena is deeply experienced in board-level consulting and senior executive talent management in the technology sector with expertise in the semiconductor and smart devices segments.

Kristi Maynor
Dallas
kristi.maynor@egonzehnder.com
r +1 972 728 5935

Kristi Maynor is a consultant in the Dallas office of Egon Zehnder and is a core member of the firm's Consumer, Technology and Communications Practice Groups. Kristi also is a member of our Diversity and Inclusion specialization and provides management appraisal and accelerated integration support for clients.

Chris Patrick
Dallas
chris.patrick@egonzehnder.com
+1 972 728 5950

Chris Patrick, based in Dallas, is a trusted advisor for CIO and C-suite talent strategy and development for global companies across a diverse set of industries, including retail/consumer products, IT services, industrial, financial services and digital. As the Global Leader for Egon Zehnder's Chief Information Officer Practice, Chris advises some of the world's leading corporations on talent development and assessment at the board-level and across the executive suite.

Egon Zehnder is the world's leading privately held executive search and talent management consultancy with more than 400 consultants in 69 offices across 41 countries. The firm provides senior-level executive search, board search and advisory, CEO succession and family business advisory, as well as leadership assessment and development to the world's most respected organizations. Egon Zehnder's clients range from the largest corporations to emerging growth companies, family and private-equity controlled entities, government and regulatory bodies, and major educational and cultural organizations. For more information: www.egonzehnder.com.

Amsterdam
Athens
Atlanta
Bangalore
Barcelona
Beijing
Berlin
Bogotá
Boston
Bratislava
Brussels
Budapest
Buenos Aires
Calgary
Chicago
Copenhagen
Dallas
Dubai
Düsseldorf
Frankfurt
Geneva
Hamburg
Helsinki
Hong Kong
Houston
Istanbul
Jakarta
Jeddah
Johannesburg
Kuala Lumpur
Lisbon
London
Los Angeles
Luxembourg
Lyon
Madrid
Malmö
Melbourne
Mexico
Miami
Milan
Montreal
Moscow
Mumbai
Munich
New Delhi
New York
Oslo
Palo Alto
Paris
Prague
Rio de Janeiro
Rome
San Francisco
Santiago
São Paulo
Seoul
Shanghai
Singapore
Stockholm
Stuttgart
Sydney
Tel Aviv
Tokyo
Toronto
Vienna
Warsaw
Washington, D.C.
Zurich