Severe Cyber-Attack Predictions for 2019

By Tony Chapelle March 4, 2019

2018 was a bad year for data breaches. Besides the inexorable growth in cyber attacks, a major regulator and even a proxy advisory firm took action against firms that didn't make sufficient progress — or effort — in getting a handle on cyber security and data privacy.

That makes this a crucial year for corporate boards to understand and implement better information governance.

Tech and governance experts are predicting advanced forms of breaches in 2019 that will only compound cyber woes for companies that are unprepared. (Please see sidebar.) Some of those include a public cloud vendor being breached and attacks on companies through printers. For example, last year, fans of one of YouTube's top-ranked entertainers, called **PewDiePie**, found they could attack random corporations through their printers and send printouts touting the star's show.

Breaches that Affected the Most Users in 2018

Marriott International/Starwood	500 million guests
Exactis	340 million records
Under Armour	150 million MyFitnessPal records
My Heritage	92 million records
Panera Bread	37 million customers
Facebook	50 million hacked users plus 40 million Facebook View users 30 million access tokens
Ticketfly	27 million accounts

Source: Fox Rothschild law firm

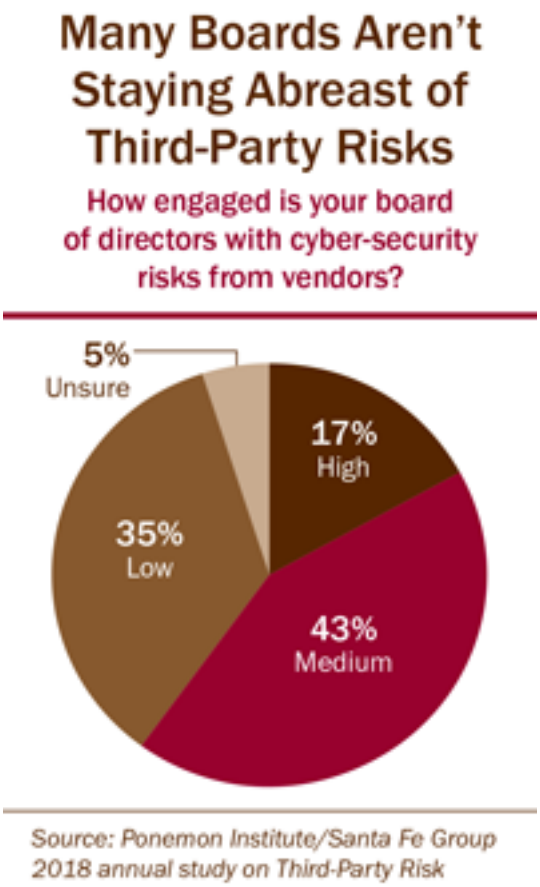
"Many boards do a better job of managing their children's elementary school grades than their companies' digitization and cyber security for which they have fiduciary responsibility," maintains

George Wrenn, founder and CEO of **CyberSaint Security**, a compliance and risk management consulting firm.

“Is your board asking for qualitative and quantitative monthly reviews about your cyber posture? If a board doesn’t treat and talk about cyber security like a business function the same as financial reporting or filing taxes, it won’t make resources available to implement effective security.”

Last April, the **Securities and Exchange Commission** for the first time fined a company — **Altaba**, formerly known as Yahoo — for waiting two years to notify users their personal information had been compromised. Last March, **Egan-Jones Proxy Services** became the first proxy advisory shop to **recommend withhold votes for board directors** based on testing the board companies’ domain name systems (DNS) and finding them vulnerable.

What do executives and board directors need to do to “future-proof” their companies against cyber attacks in 2019?



The best safeguard, Wrenn says, is for companies to adopt the **Framework for Improving Critical Infrastructure Cybersecurity** that President **Barack Obama** commissioned the **National Institute of Standards and Technology** to create five years ago. This voluntary framework consists of standards, guidelines and best practices to manage cyber-security-related risk. Version 1.1 was released last April.

Wrenn says the NIST standards can be future-proofed — and so, by extension, can a company — if data managers use the framework to identify their risks. He advises implementing the most recent NIST cyber-security framework (CSF) and directing IT leaders to maintain the crowd-sourced controls submitted by some 300,000 tech professionals and academics. Similarly, he suggests companies can participate in the NIST CSF working group and respond to NIST's frequent "Request for Comments" bulletins.

Meanwhile, **John Nackel**, a director at **Ensign Group**, a chain of nursing and rehabilitation homes, writes in an e-mail that "the real game changer in cyber security is using artificial intelligence."

Nackel explains that, with AI, companies can analyze massive amounts of risk issues, risk data, malicious files, suspicious IP addresses, and relationships between types of threats. "It also assists with speeding up responsiveness to risk issues."

Nackel was formerly the global managing director of **EY**'s health care consulting practice and is now chairman and CEO of health care consulting firm **Three-Sixty Advisory Group**. He's keenly aware of the financial as well as reputational havoc that attacks wreak on companies. He advises boards to press managers about their cyber-security architecture, penetration tests, and policies for handling incidents and responsiveness after attacks.

Related Content

- February 25, 2019 Investors to Ramp Up Proposals on Cyber Security
- December 14, 2018 Cyber Accountability: Execs Could Face Jail
- May 7, 2018 SEC Fine Over Yahoo Breach Marks Tougher Stance on Cyber Disclosure

It's probably not surprising that finance and health care are the sectors that credit-rating agency **Moody's Investors Service** cites as having the highest exposure to cyber risk. Of all threats that have material impact on companies' financial profiles, Moody's says, data exposure and business disruption are the worst.

“Not many boards are looking at the potential financial impact of those,” says **Derek Vadala**, the global head of cyber risk for Moody’s and its former chief information security officer (CISO).

Vadala recommends that boards ask whether senior executives are aware of the technical deficiencies, or outdatedness, of their software and hardware. One alternative he suggests is forced maintenance through cloud technology, or software as a service (SaaS).

Next, he advises that firms build in security features at the outset of building IT applications. Third, he reminds that companies should test their defenses and deficiencies using the company’s security team, which should be independent of the information technology team. These independents should regularly report to the C-suite and board. Finally, boards should have a complete response plan already prepared and known by the security team, legal department and senior management in the event of a cyber incident.

“The senior team should join in a tabletop exercise on that plan once a year, and the board should receive a readout at least annually,” concludes Vadala. (For more predictions from Juniper, listen to **podcast**.)

Indeed, several experts hammered on the need for technical specialists to get face time with the board.

“If a CISO is not sitting at the CEO level, the board should have concerns about potential security incidents,” says **Mounir Hahad**, who is the head of the **Juniper Networks** research arm, Juniper Threat Labs. His colleague **Laurence Pitt**, the security strategy director at Juniper Networks, reinforced that opinion. “One of the best [phrases] I’ve heard is that the CISO is there to provide actionable security insights to the board to enable them to prepare their security investments for the future.”

Board member **Catherine A. Allen**, who also produces certification programs and sponsors research studies on cyber breaches, concurs on the need for boards to take on savvy advisors.

Allen encourages boards to appoint a digital director who can help get fellow directors up to speed on hacking, privacy and cyber security. “Having the first such director is very important,” she says.

Allen, who sits on the boards of **Synovus Financial** and **El Paso Electric**, says she’s concerned about a gamut of nation-state and hacktivist threats, including the ability of bad actors to hack into low-level internet of things devices that could connect to larger corporate

networks. Her company, **Shared Assessments**, has begun a working group to research that threat.

“Your chief risk officers ought to be doing scenario planning and start by asking the question, ‘What’s the worst thing that could happen?’” she says.

New Threatscape Predictions for 2019

Severe, emerging hacking threats to expect in 2019, according to cyber-security expert **Scott Vernick**, partner at law firm **Fox Rothschild**:

- The incidence of biometric hacking will increase.
- Expect cyber attacks on car control systems.
- Attackers will hold the internet hostage.
- A top computer cloud vendor’s system will be breached.
- A large breach will be launched through printers.
- An attack on a major wireless carrier will impact iPhones and Androids.

Here are some additional threats that tech professionals warn boards to prepare for this year.

Catherine A. Allen

Director at **Synovus Financial** and **El Paso Electric**; chairman and CEO, **The Santa Fe Group**

“Nation-states taking the electrical grid offline is an emerging threat this year. Sometimes procurement officers who make purchases on behalf of the company don’t talk to the cyber people [beforehand], and they bring in [hardware or software] products that don’t meet up to [best-practice security] standards. As a precaution, in the utility industry, the **Federal Energy Regulatory Commission** is mandating that any company that attaches any device to the grid must know where it was built and if there are any back doors on it.”

Mounir Hahad

Head of Juniper Threat Labs

Laurence Pitt

Security strategy director, **Juniper Networks**

“We predict more ransomware and phishing. They’re attacks that have been around for a long time, but they’re major threats, especially now with artificial intelligence.

“[Also,] crypto-mining will become a ride-along activity during attacks. Crypto-mining by itself won’t sustain revenue requirements for a lot of criminals, so they will move back to using ransomware or other types of attacks for intellectual property theft. They’ll implant ransomware, and, on the way out, they’ll leave some crypto-mining [implants] behind.”

George Wrenn

Founder and CEO, **CyberSaint Security** compliance and risk management firm

“I predict more cyber-kinetic attacks. Hackers used to steal credit card numbers over the computer. With cyber-kinetic attacks, we’ll see more events that cause a dam to open or a train or airplane to get rerouted. These will have physical effects on people and property.

“You’ll also see an increase in psychological operations, or PSYOPs. [These influence] populations to do what you want them to do or stop doing something they’re already doing. The Russian involvement in **Facebook** to influence the U.S. elections was a very small case. This is a growing trend by nation-state actors. It’s a very inexpensive way to project force without having to buy expensive military hardware like F-15s.”