CYBERRISKS+LIABILITIES

January/February 2018

IN THIS ISSUE

hierl

Troubling Lack of Cyber Concern by CFOs

Gone are the days when chief financial officers (CFOs) solely had to focus on managing their organization's financial risks. These days, CFOs need to think about the costs of cyber security as well as the costs associated with not having enough of it. When their security tools are inadequate or threats go unnoticed, there is an increased risk of incidents that can costs thousands or millions of dollars in repairs, lost business and reputation. CFOs need to apply new strategies when it comes to tackling cyber risks.

Work With the Chief Information Security Officer

According to recent data, 39 percent of IT workers don't believe their senior management understands the impact that a security breach could have on their company's reputation. CFOs should become active members of their security teams, instead of passive observers, in an effort to protect their revenue with a more focused and effective cyber security plan. The most effective partnerships involve weekly cyber exposure reviews with management and IT.

Invest in IT

A recent report found that firms that invest more in IT security experience an average of 6.8 fewer breaches and save more than $5 million. With the growing number of available devices that employees can use to stay connected and do their jobs, new approaches are needed to deal with increased cyber exposure that may have been more easily contained in the past.

Be Accountable

CFOs need to realize how cyber risk affects financial risk. According to a recent study by Ponemon Institute, data breaches result in an average stock price decline of 5 percent and an average revenue decline of $3.4 million. CFOs cannot manage risks of that magnitude by themselves. It is in the best interest of the entire company if its CFO partners with others in the organization who have a vested interest in managing cyber risk.

The Biggest Cyber Security Disasters of 2017

Like 2016 before it, 2017 was not without its share of cyber security incidents—incidents that impacted companies of all sizes and affected multiple industries. The following are some of the biggest cyber security disasters of 2017:

- **WannaCry**—Using a tool that was allegedly stolen from the U.S. National Security Agency, cyber criminals exploited a flaw in Microsoft's Windows system in order to spread malware dubbed WannaCry. The attack, which took place May 12, 2017, has impacted over 200,000 users in at least 150 countries.
- **Equifax**—In September of 2017, Equifax, one of the largest credit reporting agencies in the United States, was the victim of a massive cyber attack. This attack compromised the personal information of over 143 million people.
- **Yahoo**—In late 2016, Yahoo reported more than 1 billion user accounts were impacted by a 2013 breach. Later in 2017, it was revealed that over 3 billion Yahoo accounts were compromised.
- **Verizon**—In July of 2017, it was reported that 14 million Verizon subscribers may have been affected by a data breach. The majority of those impacted by the breach were individuals who had previously contacted Verizon customer service.
- **Gmail**—In May of 2017, it was revealed that Gmail users were targeted in a sophisticated phishing scam. The scam sought to gain access to accounts through a third-party app. Over 1 million users have been impacted.

Trump Administration Releases Rules on Disclosing Cyber Flaws

The Trump administration publicly released its rules on whitehouse.gov for deciding whether to disclose cyber security flaws or keep them secret. In doing so, the administration hopes to bring more transparency to its cyber processes.

The U.S. government initially created the Vulnerabilities Equities Process (VEP) under former President Barack Obama, to determine what to do with discovered flaws. The process was designed to balance law enforcement's and U.S. intelligence officers' desires to hack into devices with the intention to warn manufacturers of the need to patch holes in their security. However, the government has attracted criticism for jeopardizing internet security by stockpiling detected cyber vulnerabilities in order to preserve its ability to launch its own attacks on computer systems.

The new Trump administration charter explains how the VEP functions and names the agencies involved in the vulnerability reviews, including intelligence agencies as well as several civilian departments that include the Departments of Commerce, Treasury, Energy and State.

The National Security Agency is the executive secretariat of the interagency group. Its job is to coordinate debates over flaws that the various agencies submit in case there is a disagreement about whether to disclose them. If the disagreements cannot be reconciled, the group will vote on whether to disclose or retain the flaws.

The new rules also require the creation of an annual report to provide metrics on the amount of flaws discovered, retained and disclosed. Portions of the report are to be made public. Decisions to retain vulnerabilities are to be reconsidered every year.

According to White House security coordinator Rob Joyce, the revised rules are intended to shed light on the process for how various federal agencies weigh the costs of keeping a flaw secret. Joyce said the rules are the most sophisticated in the world and that they set the United States apart from most other nations.

More than 90 percent of flaws are ultimately disclosed, according to Joyce, although critics argue that they're not shared quickly enough.

Hierl Insurance Inc.
[B_Number_Street]
[B_City_Town], [B_Postcode]
920-921-5921
www.hierl.com