CYBERRISKS+LIABILITIES

IN THIS ISSUE

McAfee Report Projects Top Cyber Threats of 2016

The McAfee Labs 2016 Threat Predictions report identifies top threats for the coming year as well as predictions for future cyber threats through 2020. The following is a summary of the report's findings:

- **Hardware:** Attacks that exploit flaws in both hardware and firmware components are expected to continue; security experts recommend being mindful of this potential avenue of exploitation below the level of the operating system.
- **Ransomware:** Ransomware attacks will likely become more common and more sophisticated. "Ransomware-as-a-service" is expected to continue growing, which will allow inexperienced cyber criminals access to the ransomware. Additionally, experts predict that ransomware will expand beyond Windows and also start targeting the increasingly popular Mac OSX.
- **Wearables:** Wearable devices are becoming much more popular. While these devices don't store very sensitive data themselves, they do connect to smartphones via Bluetooth, offering criminals a new potential "back door" into a user's smartphone. The report suggests that cyber criminals might, for instance, use GPS data gathered from a user's fitness tracker to create spear-phishing email attacks that the user is more likely to open.
- **Automobiles**: Wired magazine stunned the automotive world in July 2015 when it ran a feature story outlining how a couple of enterprising hackers remotely commandeered a Jeep Cherokee. Experts predict a rise in the number of exploited zero-day vulnerabilities, but even identified threats pose a problem, because some companies cannot issue remote updates to certain car models.

(continued on the next page)

Target Agrees to Pay a Nearly $40 Million Settlement

Target has agreed to pay $39.4 million to settle a class-action lawsuit stemming from its 2013 data breach. The suit was filed on behalf of card issuers, banks and credit unions that had to give new cards to customers after their data was stolen from the retailer. This is just one of a number of lawsuits that have been filed since the data breach, and Target claims that it's paid about $290 million in costs related to the breach.

Survey Finds Global Companies Worried About Cyber Threat Detection and Defense

According to EY's Global Information Security Survey (GISS) 2015, "Creating trust in the digital world," 88 percent of global organizations believe that their information security architecture doesn't meet their current security needs. In fact, 36 percent aren't confident that they even have the ability to detect sophisticated cyber attacks.

When asked about the source of cyber attacks, respondents named criminal syndicates (59 percent), employees (56 percent) and hacktivists (54 percent) as their top concerns. To meet this threat, 69 percent of respondents said that they'd like to increase their cyber security budgets by as much as 50 percent.

Cyber Information Sharing Act Passed as Part of Spending Bill

The Cyber Information Sharing Act (CISA), a significant piece of cyber security legislation, was added to the omnibus spending bill passed by Congress and signed into law by President Barack Obama last month. CISA is designed to encourage companies to cooperate with one another and with governmental agencies when disclosing and sharing information about identified cyber security threats, in part, by offering immunity to companies as a result of sharing that information. Proponents of CISA say that sharing information will allow both the government and the private sector to respond to threats more quickly and efficiently. Critics, however, worry about the privacy of sensitive customer and patient data.

Top Cyber Threats of 2016

(continued from the previous page)

- **Integrity:** Integrity attacks represent a new, and potentially costly, type of cyber attack that most companies have seen in the past. Unlike other cyber attacks in which criminals simply damage or steal data, integrity attacks involve criminals selectively and surgically altering data in communications or transactions in ways that benefit them. Experts anticipate integrity attacks will heavily affect the financial sector in 2016 as criminals find methods of intercepting and redirecting their targets' legitimate transactions to their own bank accounts.

The report also mentioned that employees' home systems, Cloud services and cyber espionage are likely cyber threats in the coming year. Regardless of the source, it's clear that guarding yourself from cyber attacks involves identifying your exposures and developing strategies to protect yourself from each developing risk. Contact your advisor at Huckaby & Associates today to ensure your cyber risks are appropriately covered.

Moody's to Consider Cyber Attacks in Credit Assessments

Moody's Investors Service announced recently that cyber attacks are becoming a larger part of the agency's credit assessment and analysis processes. While Moody's made it clear that it doesn't consider cyber risk a principal credit factor, the agency has begun assessing cyber attacks as "event risks." An event risk is a rare but potentially severe risk, much like a storm or other natural disaster that the company includes in its stress tests as it runs its credit analyses.

The growing number and severity of cyber attacks have made such a move necessary, as companies find themselves sometimes paying hundreds of millions of dollars to counteract the damage of a single data breach. Moody's has released a report highlighting three important areas for companies to think about when considering the credit impact of a cyber attack:

- The type and importance of the affected asset or business
- The duration of the service disruption
- The scope of the business or assets affected by the cyber attack

For help assessing your cyber liabilities, contact Huckaby & Associates today.

Huckaby & Associates
P.O. Box 21154
Columbia, SC 29221
(803) 772-3773
www.huckabyandassociates.com