CYBERRISKS+LIABILITIES

March/April 2018

IN THIS ISSUE

Cyber Criminals Stole Almost $20 Billion from U.S. Consumers in 2017

According to Symantec's 2017 Norton Cyber Security Insights Report, more than one-half of the adult internet population in the United States was affected by some form of virus, malware, spyware or phishing scam in 2017. That accounts for roughly 143 million Americans. From those attacks, consumers lost $19.4 billion, and the average cyber crime victim spent 23.6 hours dealing with the aftermath.

Many of the crimes resulted from consumers making basic security mistakes. For example, 60 percent of victims made the mistake of sharing at least one of their passwords for their online accounts or devices with another person. Another cyber mistake was using a single password across multiple online accounts, which is something 24 percent of U.S. consumers made the mistake of doing, according to the survey.

The group of U.S. consumers with the best password management was the baby-boomer generation, with 69 percent ensuring they used a different password for each online account. However, 24 percent of them made the mistake of writing down their passwords on a piece of paper.

Prevention is Key

Symantec recommends following these basic cyber security best practices to ensure safety online:

- Change your passwords every few months.
- Don't use the same passwords for multiple accounts.
- Don't share your passwords.
- Use an anti-virus program.
- Use due diligence when opening emails, clicking on links or downloading attachments online.

hierl

Cyber Tops List of Threats to United States

Cyber was at the top of the list of worldwide threats at a Senate Select Committee on Intelligence hearing on Feb. 13, 2018. Daniel Coats, the director of national intelligence, discussed a cyber war that nations, organizations and sometimes individuals are fighting against the United States, stating that the nation faces a complex, volatile and challenging threat environment with the risk of interstate conflict higher than it has been since the end of the Cold War.

Reasons Cyber is Considered a Top Threat

Coats said adversaries try to use cyber attacks to divide the United States and weaken its leadership. The countries that pose the largest cyber threats are Russia, Iran, China and North Korea, according to Coats, and each of those countries has the intent to degrade our democratic values and weaken our alliances.

Type of Threats by Country

During the intelligence hearing, the director described the types of threats by country as well as the reasons for them. For example, China has historically used cyber attacks to support its national security and economic priorities. Iran has tried, and will continue to try, to penetrate U.S. and allied networks for espionage and lay a foundation for future cyber attacks. North Korea will continue to use cyber to raise funds, gather intelligence and launch attacks against the United States.

Coats also stated that the United States, along with its European allies, should expect persistent and disruptive cyber operations to continue against them. In the United States, this includes businesses as well as federal, state and local governments.

6 Cyber Security Topics to Watch in 2018

Business and government leaders need to be on constant alert for cyber attacks of all types. With the evolution of cyber threats each year, there are specific threats to focus on for 2018. Here are six cyber security trends to watch in 2018:

1. **Cryptocurrency**—This is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. With many people interested in ways to capitalize on cryptocurrency, it is important to realize that the market is very volatile and highly susceptible to fraud and cyber attacks. Some experts feel the cryptocurrency market needs better security and a way to guarantee losses from theft.

2. **Artificial intelligence (AI)**—Approximately 87 percent of U.S. cyber security professionals use AI software to identify and predict cyber threats. However, AI can also be used by cyber criminals against the same organizations that use it for protection.

3. **More multifactor authentication**—Even though many companies fear that implementing multifactor authentication would negatively affect user experience, the growing concern about stolen passwords might convince them to implement it.

4. **Increased regulation**—Businesses could face increased regulation as governments try to compete with the growing risk of data breaches and attacks on infrastructure. One example of such government efforts is the General Data Protection Regulation in Europe.

5. **Increase in state-sponsored attacks**—Such attacks tend to be politically motivated. Instead of focusing on financial gain, the intent of these attacks is to acquire intelligence that can be used to obstruct the objectives of a political entity. Appropriate efforts to deter and respond to these attacks will be a key topic for policymakers and businesses over the next decade.

6. **Increasing demand for a chief information security officer (CISO)**—Due to the shortage of skilled cyber security professionals, many companies hire external cyber security services and virtual CISOs. This outsourcing is expected to continue until employers find ways to fill the skills gap.

Hierl Insurance Inc.
325 Trowbridge Drive
Fond du Lac, WI 54937
920-921-5921
www.hierl.com