Cyber Risks & Liabilities

First Quarter 2019

Top Cyber Predictions for 2019

The average global cost of a data breach has risen to $3.86 million, magnifying the need for companies to be aware of all potential threats. Here are just a few of the threats that cyber security experts have forecast for 2019.

Artificial Intelligence (AI) as a Weapon

With AI being so young, it is still vulnerable to attacks that can affect its operations. However, AI could also be used defensively to identify new threats and better protect systems from attacks.

A Lack of Security in the Cloud

As organizations are adding more data to the cloud, they're not practicing good enough housekeeping to secure that data, making them a top target for cyber criminals.

5G Network Vulnerability

As 5G takes the place of 4G, the market for 5G infrastructure is expected to grow by 118 percent annually through 2022. Although that rate of growth may be profitable for cellular networks and providers, it creates new vulnerabilities as well. Instead of connecting to a Wi-Fi router, 5G devices are expected to connect directly to a 5G network, making those networks more appealing targets to hackers while also making it more difficult for home and office users to monitor their devices.

Biometric Hacking

Despite being the most secure method of authentication, biometric data can be stolen and altered. And sensors on smart devices can deteriorate with excessive usage, making them less reliable and easier to hack.

Skimming Magnified

Criminals are targeting bank networks with malware, similar to the way they use credit and debit card skimmers to steal banking information and passcodes from unsuspecting customers. The result can be millions of dollars in losses and a lack of trust in major financial institutions.

Online Gaming

The online gaming industry has seen massive growth and is expected to hit $2.2 trillion by 2021. This is an attractive target for cyber criminals who can easily pose as gamers and gain access to their credit card information.

More Targeted Spear Phishing

Devious cyber criminals are using tactics that involve breaking into an email system and learning as much as they can about their targeted victims. They use that information to take advantage of the trust built with another person and scam them out of money.

HUCKABY & ASSOCIATES | HIIB GROUP

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

New Sanction Retaliations from Iran Worry U.S. Banks

After the Trump administration reimposed the sanctions lifted as part of the 2015 Iran nuclear deal, U.S. banks are expecting retaliation in the form of cyber attacks.

The Treasury Department added 700 entities to the list of reinstated sanctions, including Iranian banks, aircraft, vessels, individuals and the country's energy sector.

According to recent reports, a major U.S. bank, which chose not to be identified, listed Iranian hackers as the top trending cyber threat, even ahead of North Korea.

The entire banking industry is on alert after the Iranian government issued public statements intending to defy the sanctions. When asked about the threat, the CEO of the Financial Services Information Sharing and Analysis Center—the privately run group that coordinates defenses against cyber attacks—stated that he was more confident in the organization's ability to ward off Iranian cyber attacks than when Iran targeted U.S. banks in 2011.

From 2011-2013, Iran launched a series of cyber attacks, jamming the internet services of major U.S. banks with garbage computer traffic. Instigated by seven Iranians on behalf of the Islamic Revolutionary Guard Corps, the cyber attacks were unprecedented in size.

Experts at cyber security firm CrowdStrike worry that the Iranian hackers' skills have grown since the 2011-2013 attacks. Although banks are at the top of the radar, every type of business is vulnerable to cyber attacks, magnifying the need for adequate cyber security.

How to Secure Office IoT Devices

An internet of things (IoT) device is any smart device that is connected to the internet. Many of these devices are everyday objects—like watches or thermostats—that connect via Wi-Fi, allowing users to control them remotely or even collect data.

Employers pride themselves on using IoT technology to make their workplaces more modern and help them stand out from their competitors. Things like smart desks, video conferencing systems, security systems, smart TVs and intelligent HVAC systems are becoming more commonplace. Unfortunately, these same gadgets, as well as other IoT devices, can create a growing security threat for businesses who aren't prepared.

There is a lack of consistency between manufacturing companies who make the IoT devices. They have different operating systems and different security measures, and some aren't even capable of software updates. This makes it difficult for IT departments to prevent hackers from accessing IoT devices and gaining access to company networks.

That's not to say that your organization shouldn't use IoT devices altogether. You just need to take extra precautions. Here are a few ways to protect your valuable data while reaping the benefits of IoT devices:

- **Consider multi-factor authentication or use certificates.** Both are able to stall hackers who've managed to crack your password.
- **Create a separate Wi-Fi network specifically for all IoT devices.** If hackers access the IoT network, your separate business network should still be safe.
- **Limit access to sensitive data.** For example, IoT security cameras can expose sensitive information to hackers. Therefore, it is important to consider what the device has access to before setting it up. Be sure to also clear its storage on a regular basis. In addition, it's important to never store critical business or personal data on these devices.
- **In the event of a hack, be prepared to disable your devices and reset the factory settings at any time.** If you regularly back up your devices, it should be easy enough to restore them and reconnect.
- **Avoid installing third-party software**. It's easy to add functionality to IoT devices simply by installing additional applications. However, you should never install software from an untrusted source. Doing so can open the door to hackers.
- **Turn off IoT devices when they aren't in use.** This may seem like a simple solution, but active devices are vulnerable to attacks. Just by switching off unused devices, you can improve network security overall.

Although IoT technology is likely here to stay, it is important to remember that it is still in its infancy. By taking proper precautions, you can enjoy its conveniences instead of letting it threaten your business operations.

This Compliance Bulletin is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.