CYBERRISKS+LIABILITIES

IN THIS ISSUE

JRG
ADVISORS

New York Cyber Rules May Become Model for Other States

In recent statements by New York's financial regulator, a group of U.S. state insurance regulators have been advised to use the state's groundbreaking cyber security rules as a model for how financial institutions and insurers should protect their networks from hackers and disclose cyber events.

The superintendent of the New York State Department of Financial Services called the regulation "a road map with rules of the road," which can provide a uniform cyber security law that all states can choose to adopt for use by financial institutions and insurers to focus on cyber security threats.

New York's cyber security rules took effect on March 1, following a series of data breaches that resulted in losses of hundreds of millions of dollars to U.S. companies that included Home Depot Inc., Target Corp. and Anthem Inc. The new rules describe steps that covered entities must comply with in order to protect their customer data and networks from cyber criminals.

One such rule calls for firms to scrutinize the security of third-party vendors that provide them with goods and services. They must also perform risk assessments in order to design cyber security programs particular to their specific needs. All covered entities are required to certify compliance annually.

A proposed model cyber security law that all states can choose to adopt for financial institutions and insurers could lead to more uniformity among states. But they first must be finalized and approved by a task force of state insurance commissioners before being considered by state lawmakers. However, since the task force's inception in 2015, insurance commissioners haven't been able to agree upon several points of the law. A fourth draft is expected by May 9.

For more information regarding New York's cyber security laws, see "New York Cyber Security Laws – Cyber Security Program Rules" and "New York Cyber Security Laws – Covered Entity Responsibilities."

Most Employees Breach Network Security

A recent cyber security report indicated that 95 percent of organizations have workers who try to override security and web restrictions—behaviors that may lead to data theft and other malicious activity in the workplace. The report warns employers about workers who use anonymous VPNs, which is a practice that has doubled between 2015 and 2016.

According to the report, employees attempt to override security restrictions so they can steal data, shop online or cover up prohibited internet searches. However, most employee cyber security incidents—almost 90 percent—happen by accident.

Even with policies and enforcement procedures in place, workers typically find ways to break through security systems if they're persistent. In order to prevent data breaches, employers should increase visibility during on- and off-network times, pay extra attention to workers who violate policies and train IT staff in high-level security.

FBI May Ease Cyber Employment Standards

In an effort to recruit much-needed cyber security agents, FBI Director James Comey is considering loosening certain training requirements on marksmanship and physical fitness for its cyber security applicants.

One possible solution in consideration is to create a special university for the training of cyber security agents who wouldn't necessarily need to carry a gun. The cyber university could be a workaround to the current FBI requirements and would serve as a place to teach agents required technical skills for the job.

Another possible solution is to scrap the requirement that requires agents who've left the service for more than two years to re-enroll in the FBI's training academy.

Using a VPN to Protect Browsing Data

The U.S. House of Representatives recently voted to reverse regulations that would have prevented internet service providers (ISPs) from selling users' web-browsing data without their explicit consent. The decision has left people wondering how to prevent big telecom companies from making money off of their web-browsing data. One solution may be to use a VPN.

What is a VPN?

A VPN is a private, controlled network that connects users to the internet. The connection with the VPN's server is encrypted, thus making the data confidential while being transported. In short, a user's connection to a VPN remains private even though the data being transmitted moves over the notoriously public internet.

How Does a VPN Protect User Data?

If you use public, unencrypted Wi-Fi at places such as airports, coffee shops or hotels, you put your privacy at risk. But if you connect to a VPN immediately after connecting to its Wi-Fi, you can surf more safely.

VPNs also keep ISPs in the dark as to what their users are doing while online. The ISP can see that there is a user, but it can't see what the user is doing online. Some VPNs even allow their users to hide their physical location in order to gain access to geo-restricted content from video-streaming sites.

Are VPNs Reliable?

Using a VPN can enhance your privacy and security, but you should never assume that it is foolproof. A VPN has the potential to do the reverse of what it is intended for, as it can access and track all of your online activities and browsing history. It should also be noted that using a private VPN in the workplace can violate internet policies and be grounds for termination.

For a VPN to provide more privacy than an ISP, you need to confirm that the company offering the VPN is trustworthy, which can be a difficult thing to prove. One indicator of trust is whether the VPN keeps logs of user activity. Still, a company that provides VPNs could misrepresent its practices or accidentally store data for longer than it claims to, rendering the provider's promise useless.

One way to ensure the reliability of a VPN is to pay for it instead of opting for a free version. A provider that offers VPNs for free may not be able to afford the resources needed to offer the security features it claims to offer.

JRG Advisors, LLC
7000 Stonewood Drive, Suite 251
Wexford, PA 15090
412-456-7000
http://www.jrgadvisors.net/

This publication is for informational purposes only. It is not intended to be exhaustive nor should any discussion or opinions be construed as compliance or legal advice. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.