IADC COMMITTEE NEWSLETTER

CYBER SECURITY, DATA PRIVACY AND TECHNOLOGY

May 2021

IN THIS ISSUE

Ransomware attacks have accelerated at an exponential rate as the vulnerabilities of businesses and governments have become exposed in increasingly networked environments. This article discusses the high profile cyberattacks dominating the news, President Biden's recent executive order to improve the nation's cybersecurity, and risk management steps businesses can take to reduce, if not eliminate, exposure to security incidents and breaches.

The Ransomware Scourge: Connectivity and Vulnerability in an Internet of Things, 5G World

ABOUT THE AUTHOR

David Patrón is a partner at Phelps Dunbar. As head of the firm's litigation practice, David represents some of the biggest names in technology, oil and gas, entertainment and other industries. With over 25+ years of practice, David represents and counsels clients on a wide variety of complex legal issues, including antitrust, intellectual property, e-commerce and internet use, and cybersecurity. After living on the U.S. East, West and Gulf coasts and spending significant time with extended family in Mexico, David excels at navigating diverse perspectives. He has vast experience resolving disputes at home among his five children, including two sets of twins. He can be reached at David.Patron@phelps.com.

ABOUT THE COMMITTEE

Corporations and law firms around the world are constantly dealing with cybersecurity, data privacy and other important technology issues, both in business and, where available, in litigation discovery. Burgeoning technologies are placing new and increasing demands on in house and outside lawyers and their clients. All are being challenged to meet new and strict data privacy and security guidelines and the consequences for failing to meet these requirements can be devastating. The Cyber Security, Data Privacy and Technology Committee will address the differing substantive laws globally in these areas, and be of interest to many other committees whose members and activities are impacted by technology. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Avanti D. Bakane
Vice Chair of Publications
Gordon & Rees, LLP
abakane@grsm.com

The most serious cyber threat in 2021 is ransomware, a scourge affecting commerce and national security at a blistering pace. According to Sophos' annual ransomware survey, 37% of organizations – over a third of the 5,400 surveyed – were hit by ransomware last year. 54% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data. In Congressional testimony earlier this month, Christopher Krebs, the former top cyber official in the Department of Homeland Security, told lawmakers that the ransomware emergency in the U.S. is a "digital dumpster fire."

The Never-Ending Assault on Businesses and Governments

One only has to read the headlines to see that the threat of ransomware is exploding. This month alone, thousands of gas stations have run dry following the cyberattack that forced Colonial Pipeline to shut down. The Colonial Pipeline attack has already been supplanted in the news by a cyberattack on the Irish health service computer systems, which has been described as "possibly the most significant cybercrime attack on the Irish state." Only a few months ago, a global wave of cyberattacks and data breaches began after exploits were discovered in on-premises Microsoft Exchange Servers, giving attackers full access to user emails and passwords, administrator privileges, and connected devices on the same network. These high profiles attacks came on the heels of the SolarWind attack where hackers used a routine software update to slip malicious code into software produced by SolarWinds and then used it as a vehicle for a massive cyberattack.

These recent cybersecurity incidents are a sobering reminder that public and private sector entities increasingly face sophisticated malicious cyber activity. These incidents share a common cause -- namely, insufficient cybersecurity defenses that leave public and private sector entities vulnerable to cyberattacks. Indeed, the prolific payment of ransoms has caused a snowball effect, encouraging even more ransomware attacks.

Planning for Future Cyberattacks: A Federal Response

In response to these high profile attacks, President Biden signed an Executive Order on May 12, 2021 to improve the nation's cybersecurity and protect federal government networks. The Executive Order improves software supply chain security by establishing baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.

The Order also modernizes and implements stronger cybersecurity standards in the federal government by accelerating movement to secure cloud services and a zero-trust architecture and mandating deployment of foundational security tools such as multifactor authentication and

encryption. In addition to creating a standard playbook for responding to cyber incidents, the Order establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, to convene following a significant cyber incident to analyze root causes and to make concrete recommendations for improving cybersecurity.

A Growing Problem In a 5G, "Internet of Things" World

Ransomware and malware are pernicious threats due to their capacity to deny essential services and effectively shut businesses down. Their use will only proliferate with the continued ascendance of the Internet of Things (IoT), a term used to describe physical devices and equipment that can collect and share data and are locatable, addressable, and/or controllable via the Internet. IoT devices can be found in almost all aspects of modern life. It encompasses everything from smart cars, HVAC systems, and home appliances, to security cameras and wearable technology. IoT represents the melding of the physical world and the digital world, with physical objects communicating with each other including machine to machine, and machine to people.

IoT has infiltrated countless industries, including energy, manufacturing, finance, healthcare, and food production. IoT has also brought us smart homes, buildings, and even cities. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security, and environmental monitoring all are examples of IoT applications. According to The McKinsey Global Institute, 127 new devices connect to the internet every second. IoT Analytics estimates that, by 2025, there will be more than 30 billion IoT connections, almost 4 IoT devices per person on average.

The exponential growth of IoT has led to greater security and privacy risks. Many such risks are attributable to device vulnerabilities that arise from cybercrime by hackers and improper use of system resources. Each IoT device represents an attack surface that can be an avenue into your data for hackers. Unlike laptops and smartphones, most IoT devices possess fewer processing and storage capabilities. This makes it difficult to employ anti-virus, firewalls, and other security applications that could help protect them.

There is a growing rate of IoT attacks. The U.S. General Accounting Office GAO identified denial of service, malware, passive wiretapping, structured query language injection, and wardriving (search for wi-fi networks by a person in a moving vehicle) as primary threats to IoT. There have been documented cybersecurity issues with smart security cameras, including a flaw in Amazon's Ring Video Doorbell Pro, which led to a class-action lawsuit alleging that hackers were given unauthorized access to the user's Wi-Fi network and potentially to other connected devices on it. In one disturbing example straight out of a horror movie

script, a Smart Home setup was hacked by unknown intruders who played disturbing music from the video system at high-volume while talking to them via a camera in the kitchen, and also changed the room temperature to 90 degrees Fahrenheit by exploiting the thermostat.

Protect Yourself

No tactic can completely prevent a cyberattack, but basic steps can be taken to reduce your exposure by adopting a risk management approach to understanding what is connected in the IoT landscape, knowing how to best protect the most important assets, and effectively mitigating and remediating security incidents and breaches. Each device connected to a network should be configured with security in mind. NortonLifeLock Inc. recommends the following 12 basic security protections you can implement now to safeguard your IoT devices:

- Give your router a unique name
- Use a strong encryption method for your Wi-Fi
- Set up a Guest Network for your friends to keep your personal Wi-Fi network private
- Change default usernames and passwords
- Use strong, unique passwords for Wi-Fi networks and device accounts
- Check the settings for your devices
- Disable features you don't need
- Keep your software up to date
- Audit the IoT devices already in use on your home network
- Implement multifactor authentication
- Avoid public Wi-Fi networks
- Watch out for power outages to prevent your devices from falling into an unsecure state

There is no silver bullet for securing IoT devices, but being more cybersecurity aware and prepared should be a priority for everyone connected.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

FEBRUARY 2021
If you Want to Stay Friends with your IT Supplier, Use the Contract!
Anna Cook and Robert Graham

MARCH 2018
First Class Action Data Breach in the UK – Employer Found Vicariously Liable for Rogue Employee's Actions
Elena Jelmini Cellerini and Vikram Khurana

NOVEMBER 2017
Blockchain Unchained: One Lawyer's Quest to Figure out what the Hell Everyone is Talking About
Kendall Harrison

AUGUST 2017
Def Con Hacker Conference: An Accidental Tourists Observations
Elizabeth S. Fitch

MAY 2017
Doe v. Backpage.com and its Aftermath: Continued Uncertainty and New Litigation in the Wake of the Supreme Court's Denial of Certiorari
David Patrón

APRIL 2017
Incorporating Technology into the Management of the Work Processes at the Firm
Donna L. Burden, Elizabeth S. Fitch and Park L. Priest

FEBRUARY 2017
"The First Thing We Do, Let's Kill All The Lawyers"
Elizabeth S. Fitch and Elizabeth Haecker Ryan

DECEMBER 2016
A Primer for Understanding Blockchain
Doug Vaughn and Anna Outzen

AUGUST 2016
The Attorney-Client Relationship in the Electronic Age
Elizabeth S. Fitch and Theodore M. Schaer

MAY 2016
Understanding the Defend Trade Secrets Act of 2016: "We're Not in State Court Anymore"
Peter J. Pizzi and Christopher J. Borchert