New York Law Journal

SERVING THE BENCH AND BAR SINCE 1888

WWW.NYLJ.COM

An ALM Publication

VOLUME 261—NO. 34

THURSDAY, FEBRUARY 21, 2019

Outside Counsel

Expert Analysis

How the Internet of Things Expands Cyber Risk Well Beyond Your Perimeter

BY TED AUGUSTINOS,
ANDY GANDHI
AND ADRIEL GINSBURG

It's an exciting Friday at the company. Months of planning an acquisition will culminate in a public announcement early the next week. In a bustling conference room, the planning team reviews the execution plan one last time. Spirits are high as the weekend approaches.

By midday Monday, the mood has drastically shifted. An early morning buying frenzy of the target company's stock inflated its price, fueling rampant speculation of an acquisition. The stock is no longer at an acceptable price and months of planning are undone. The company's executives, confident in the deal team's integrity, engage a cybersecurity firm to determine if they've been hacked.

The cybersecurity team determined the smart TV in the conference room was hacked, its built-in microphone activated and recordings of planning sessions were exfiltrated. The company carefully secured email and other traditional IT resources but overlooked the Internet of Things (IoT).

What Is 'The Internet Of Things'?

Without a universally accepted definition, IoT is generally considered the interconnection of any device to other devices or systems through the Internet. While that may seem simplistic, IoT is that all-encompassing. Examples include everything from simple household appliances to city-wide flood control and emergency response systems. The purposes for IoT can be equally varied, from reporting malfunctions in machinery to actively collecting data in smart homes and taking complex actions based on that input. According to research firm Gartner, by 2020 the total number of IoT devices on the Internet is expected to exceed 20 billion.

While the scope is vast, there are generally three types of IoT technologies:

- **Consumer:** Examples include Alexa, Google Home, automobiles, monitoring solutions and wearables. Consumer IoT tends to access a wide array of data (including audio, video, biological, medical and environmental), with widely varied cybersecurity capability. Consumer IoT often has bidirectional functionality;

TED AUGUSTINOS *is the Hartford office managing partner of Locke Lord, and a member of the Steering Committee of the firm's privacy and cybersecurity practice group.* ANDY GANDHI *is a managing director with Alvarez & Marsal's disputes and investigations practice in New York, and leads the digital investigation practice within the forensic technology services team.* ADRIEL GINSBURG *is a director at Alvarez & Marsal's global cyber risk services.*

the device not only monitors and reports but can take actions based on collected data.

- **Enterprise/Commercial:** Examples include office lighting systems, teleconferencing solutions, office monitoring solutions and medical equipment. Enterprise IoT tends to be moderately homogeneous with specific purpose and limited data. Enterprise systems tend have some limited bidirectional functionality.
- **Industrial:** Examples include fuel level monitoring, malfunction reporting, anomaly reporting and automation metrics. Industrial IoT tends to perform simpler functions with a single purpose and limited access to data. Industrial IoT is often, but not always, unidirectional reporting data back to the user but unable to take actions based on input.

How Does IoT Affect Cyber Risk?

IoT has proven to be a game changer for businesses. IoT has the power to exponentially increase productivity, efficiency, problem-solving and customer interaction, as well as to multiply their offerings of consumer devices. These benefits come with a cost. While IoT devices have a variety of uses, from automatically reordering coffee filters to immediate notification and deployment of repair crews for offshore oilrig malfunctions, there is a proportionate expansion of cyber risk. The same functionality that allows a facility manager to unlock the loading dock remotely for a delivery can also be exploited by an attacker.

IoT can affect overall cybersecurity risk on numerous levels, by introducing connectivity to unconventional operating systems that may not integrate with existing control structures, and by expanding the potential attack surface both internally and externally. As IoT technologies become mission-critical, cybersecurity risks increase in severity.

Data Risks

From a data perspective, IoT devices can collect, store and transmit sensitive data by design or in unknown ways. Passive input devices may be default configured to record all input from the area, such as video, audio and use habits, and report back to a third party.

In addition to sensitive company or personal data, IoT devices often store connection data that could be harvested while in use or when discarded. As an example, burned out smart bulbs should be securely disposed of as IoT devices, as they can hold Wi-Fi Service Set Identifiers (SSIDs) and passwords.

> IoT has the power to exponentially increase productivity, efficiency, problem-solving and customer interaction, as well as to multiply their offerings of consumer devices. These benefits come with a cost.

Additional Risks

Beyond the loss or manipulation of data, IoT can present direct threats to the public. For example, connected medical devices could be ransomed under threat of disrupting lifesaving equipment or altering medication levels. In addition to providing additional attack surface into the company, IoT could be used as an attack vehicle against others. In October 2016, attackers used a botnet built primarily of IoT devices to take down a large swath of the Internet itself.

IoT management technologies including web applications, mobile devices apps and remote access clients, all expand the attack surface and must be managed, monitored and secured.

The Compounding Effects Of Telecommuting

Telecommuting, often enabled by IoT, is rapidly growing in popularity and prevalence, but carries with it the possibility of significantly expanded cyber risk. By extending the corporate network into the home, or making it mobile, the risk and attack surfaces expand to the home and beyond as well. With exponential adoption of consumer IoT in the home, cybersecurity risks are compounded. Network security becomes a particularly heightened risk, as smart devices store network passwords, require enabling additional ports and services, and present additional points of potential compromise.

Legal and Regulatory Implications for IoT

There is much talk and some activity, but there is currently no formal U.S. legal and regulatory regime specific to the IoT environment. Certain industries have begun to craft cybersecurity guidelines, but few have developed any mature framework. While the National Institute of Standards and Technology (NIST) has issued guidance recognizing the need for an IoT security framework, no framework has been developed by NIST or similar agencies at this time.

Companies producing and deploying IoT for retail, commercial or industrial uses need to be prepared, however, as legal standards are expected. IoT developers must build cybersecurity into the development process, fully considering what information will be collected and accessed; how, where and to whom data is transmitted; and how access to the technology and information is controlled. Commercial, industrial and retail buyers of IoT need to consider the same issues, in many cases relying on the statements of sellers. Even pending the development of a specific legal framework, the accuracy and completeness of IoT disclosures will be the source of potential exposure.

Until specific IoT requirements are adopted, legal exposure will derive from existing consumer protection laws, and laws and regulations concerning the privacy and security of certain types of information. For example, the adequacy and accuracy of disclosures concerning the functionality of IoT can be expected to be reviewed under federal and state prohibitions against unfair and deceptive trade practices such as §5 of the FTC Act (15 U.S.C. §45). IoT technologies that permit access to personal information currently subject to federal and state privacy and data protection requirements will implicate data breach notification and data protection requirements, and related enforcement actions and litigation.

In addition, IoT that compromises contractual standards of data protection may create exposure to breach of contract and indemnity claims.

Risk Mitigation Strategies in The Developing Environment

Even absent a standard framework for IoT, there are several steps to be taken to identify and mitigate risk:

- **Discovery and Asset Management:** Conduct discovery exercises, such as internal and external network scans, data mapping, reviews of equipment leases, accounts payable examinations and monitoring of network traffic. Build and update a living list of IoT technologies.

Even absent a standard framework for IoT, there are several steps to be taken to identify and mitigate risk.

- **Legal, Regulatory and Contractual Compliance**: Review and monitor the developing legal and regulatory landscape, and track contracts that may impose data protection requirements. Incorporate compliance into the development, or purchase and deployment, of IoT technology.
- **Risk Assessment:** Against the backdrop of the understanding of the assets and the legal and regulatory landscape, periodically assess the cybersecurity risk associated with existing and planned IoT.
- **IoT Policy:** Develop a policy for testing, approval, use, monitoring and disposal of IoT.
- **Awareness and Training:** Incorporate IoT into the Security Awareness Program.
- **Network Segmentation:** Treat IoT technologies as an untrusted third party. Segment IoT from internal networks, restricting access to required sources, destinations, ports and services.
- **Threat and Vulnerability Management (TVM):** Incorporate IoT into TVM and patch management programs.
- **Access Control:** Restrict logical access to IoT adhering to principles of least privilege.
- **Monitoring:** Actively monitor IoT technologies at the device and network layers, where possible.
- **Device hardening:** Secure operating systems and firmware using best practice hardening standards and consider the manufacturer's reputation and cybersecurity focus when selecting IoT technology.
- **Sanitization Controls:** Securely wipe IoT devices and/or pulverize devices to prevent data extraction after disposal.

With a holistic approach to security and compliance incorporating the unique challenges of IoT, companies can develop and deploy IoT technologies in a way that delivers on the promise of IoT, while mitigating potential cyber risks and exposures.