The Internet of Everything: Building Cyber Resilience in a Connected World

The Internet of Things (IoT) is everywhere, ushering in a technological revolution at lightning speed. According to an Oliver Wyman report, between 50 billion and 100 billion devices are expected to be connected to the internet by 2020. While this rapid growth will undoubtedly open the door to new opportunities, organizations must also prepare for emerging security challenges. Are you ready for the internet of *everything*?

A WAVE OF VULNERABILITIES

IoT products are physical devices or objects embedded with electronics, software, sensors, or actuators that can connect to the internet. From refrigerators and toys to medical devices and industrial control systems, internet-connected products are transforming the way many industries do business, driving efficiency and reinventing the customer experience. IoT devices are also providing businesses with mountains of valuable data that can be synthesized with analytics to improve products, penetrate new markets, and access potential customers.

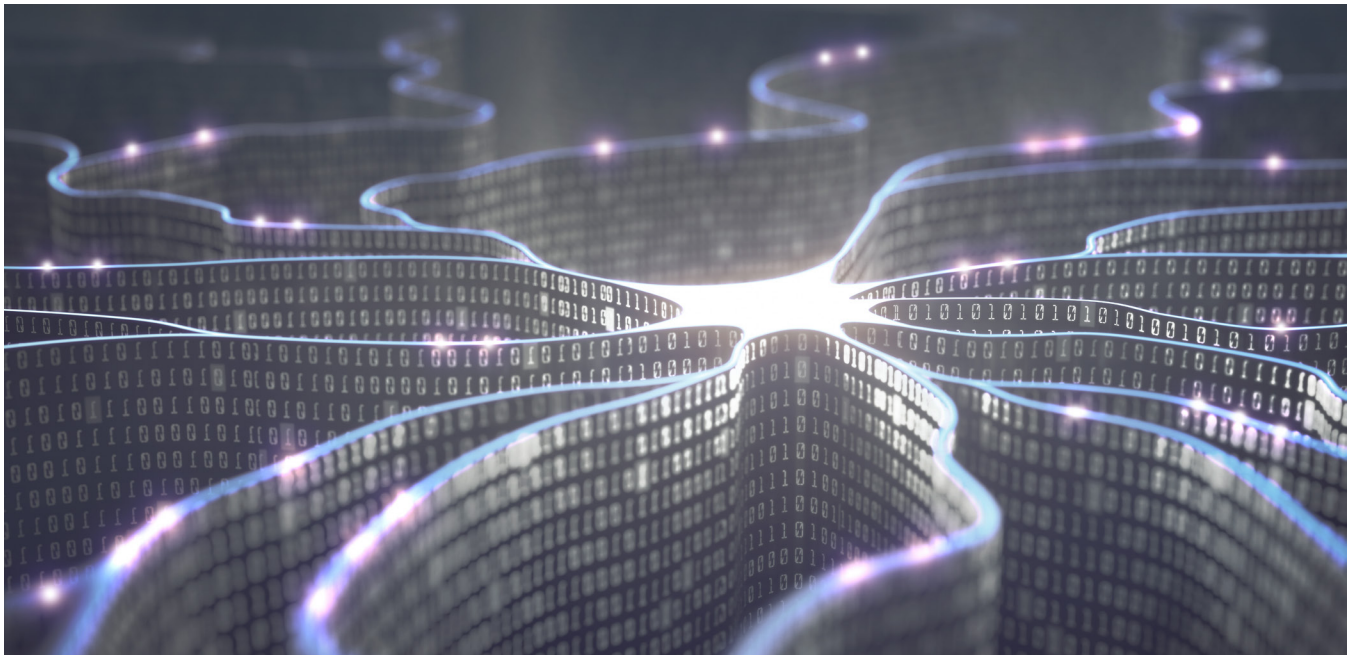
The explosion of IoT devices is dramatically changing the cyber risk landscape — and not necessarily for the better. Many security experts believe that smart devices are creating a wave of vulnerabilities because they often lack strong — or, in some cases, even basic — security features. IoT devices often also lack regular product support, such as updates and patches, making them particularly vulnerable to newly discovered weaknesses such as the *Meltdown* and *Spectre* flaws in most computer processors.

"Smart" technology is also connecting computer systems and devices that were once siloed or not directly connected to the internet. This new connectivity can leave organizations even more exposed to evolving threats that have not been fully considered or mitigated. Cybersecurity firm Symantec, for example, found that the average IoT device is attacked once every two minutes at peak times. And more than half of internet security professionals surveyed by Tripwire, a provider of integrity assurance solutions, do not feel prepared for security attacks that abuse, exploit, or maliciously leverage insecure industrial IoT devices.

"Once an IoT device is compromised," warns the FBI, "cyber criminals can facilitate attacks on other systems or networks, send spam emails, steal personal information, interfere with physical safety, and leverage compromised devices for participation in distributed denial of service

(DDoS) attacks." Recent examples of IoT attacks by malicious actors include:

- Infiltration of a North American casino's networks in 2017 by hackers who connected to an internet-connected fish tank inside the building.
- A massive DDoS attack in 2016 against a company that manages domain name server (DNS) traffic. The attackers used a botnet — a network of computers infected with malware — called Mirai to compromise internet-connected cameras across the world, which disrupted services for many of the company's customers.



A NEW IOT SOLUTION

Although IoT manufacturers and service providers cannot fully eliminate the potential for cyber and E&O claims related to their connected devices, they can secure effective insurance coverage to provide robust protection when needed. Marsh has developed a new and innovative IoT insurance product — available through Marsh Cyber CAT 3.0 as a standalone policy or by endorsement — specifically for companies that design, manufacture, and sell consumer and industrial IoT products or provide services related to those products.

Where ambiguities or exclusions may limit or preclude coverage under traditional cyber or E&O policies, Marsh's IoT product provides explicit and tailored coverage for:

- Errors and omissions in the design and manufacturing of IoT devices, including those that result in security or privacy events for customers.
- Errors and omissions in providing IoT product services.
- Extortion expenses from threats directed against or using IoT products.
- Costs or expenses to mitigate, reduce, or avoid potential claims.

Marsh's IoT product can also minimize exposures to certain risks to support expanded IoT investment and innovation accelerating your growth trajectory.

Variations of the Mirai botnet continue to wreak havoc on IoT devices. For example, earlier this year, hackers used code from the Mirai botnet and the processing power from connected devices — including smartphones and smart TVs — to mine Monero, a type of encrypted digital currency. Security experts warn that hackers will continue to attack IoT devices for crypto-mining.

Cyber-attacks that interfere with the proper operation of certain IoT devices, such as internet-connected vehicles or medical devices, may also pose a danger to human life and property. The US Food and Drug Administration, for example, has warned patients with certain heart pacemakers that they could be vulnerable if a bad actor were to send computer code to deplete the pacemaker battery or change heart rates. White-hat researchers have also demonstrated successful cyber-attacks against internet-connected vehicles.

REGULATORY CONSIDERATIONS

With a growing list of IoT attacks and warnings in the news, lawmakers have taken note. In 2017, bipartisan legislation was introduced in the US Senate to improve the security of internet-connected devices. Among other things, this legislation would require IoT vendors doing business with the US government to ensure their products meet various security requirements. Legislation designed to improve the cybersecurity of autonomous vehicles and internet-connected medical devices is also making its way through Congress. Executive branch agencies, such as the National Highway Traffic Safety Administration, are also getting involved, issuing security guidance for internet-enabled cars and trucks.

IoT regulation is not limited to the US. The United Kingdom, for example, released a report in March that sets out guidelines to help ensure IoT devices are "secure by design," with security built in from the start.

PREPARING FOR THE IOT REVOLUTION

Companies that design, develop, manufacture, or service IoT devices or products should consider a variety of potential cyber exposures. These include:

- Liability due to alleged design or manufacturing defect.
- Liability due to a connectivity failure.
- Liability due to security failure.

- Liability in providing IoT product services.
- Extortion demands against your customers or company.
- Regulatory investigations, fines, and penalties.

Companies that deploy or use IoT devices may be subject to cyber risks as well, including data breaches, business interruption and extra expense, data restoration, extortion, property damage, and bodily injury from an alleged security vulnerability or privacy breach.

To protect your business from these risks, work with your insurance advisor to assess your IoT cyber exposures and review your cyber and errors and omissions (E&O)

ASSESSING YOUR IoT CYBER RISK

Marsh Risk Consulting offers a suite of cybersecurity services tailored to an organization's technology risks, including the Internet of Things (IoT).

CYBER RISK ASSESSMENTS

Cyber risk assessments can help businesses better understand "end-to-end" risks associated with the use of IoT devices, such as automated manufacturing or production processes. We can give qualitative scores to cyber risks, in a way that easily meshes with existing enterprise risk management frameworks.

THIRD-PARTY VENDOR MANAGEMENT PROGRAM

We can work with you to conduct a detailed review of your third-party vendor management program, including continuous monitoring. This review can help you assess cyber exposures related to vendors your business relies upon for, among other things, maintenance, testing, and upgrades of mission critical industrial control systems.

CYBER BUSINESS INTERRUPTION QUANTIFICATION (CBIQ)

A CBIQ analysis of business interruption scenarios, including those driven by IoT exposures, can help you identify unresolved issues that may justify an increase in risk mitigation or risk transfer investments. This can help you understand your cyber risk exposure in financial terms and inform your decisions on cyber insurance limits, cyber mitigation investments, and risk retention.

policies to ensure appropriate coverage and limits for IoT products and services. Current policies may be silent on IoT devices and events, leaving room for ambiguities and the pervasive "silent cyber" dilemma where coverage may be available because it is not explicitly excluded. For example, technology E&O policies may have coverage available for IoT products if the definition of "technology products" is written broadly, even if that definition does not specifically include IoT products.

When reviewing your insurance policies and cyber-event response plans, consider the following questions:

- Has your organization quantified the potential losses from (or costs of) an IoT-related cyber event?
- Do your insurance policies provide sufficient coverage for a failure in the maintenance or servicing of your IoT product, such as software updates, service packs, patches, and other maintenance releases?
- Does your cyber extortion coverage include ransom demands made of customers stemming from your security or service failure?
- Do your cyber, property, and general liability policies and plans adequately protect your company from any increased cyber exposures from IoT devices?

During this review, scrutinize the wording of your policies and plans to determine whether IoT devices and services are excluded or carved out of important definitions such as "computer system," "technology product," and "professional service." Businesses should also review their property and general liability policies for coverage and keep a careful eye on relevant regulatory activity as security requirements quickly evolve to keep pace with innovation.

MARSH

For more information about IoT cyber risks and related risk management strategies, contact your Marsh representative or:

STEPHEN VIÑA
Senior Advisory Specialist
Marsh Cyber Center of Excellence
New York, NY
+1 212 345 0399
stephen.vina@marsh.com

SANDY CODDING
Managing Director
Marsh Cyber Center of Excellence
Boston, MA
+1 617 385 0277
sandy.codding@marsh.com

JOHN NAHAS
Vice President
Marsh Risk Consulting
Washington, DC
+1 202 263 7660
john.nahas@marsh.com