WHITE PAPER

IOT RISKS & REWARDS:

WHAT EVERY CXO SHOULD KNOW

IOT REWARDS ARE ALREADY HERE

The Internet of Things (IoT) is projected to generate a whopping 21% increase in corporate profits by 2022, so it's no surprise that 90% of business executives believe IoT is important to the future of their organization.[1] Benefit areas include production optimization, supply chain management, asset tracking and management, financial decision making and customer experience—with customer experience ranking number one in importance to executive leaders.[2]

By 2022, The **Internet of Things** — (IoT) — **is expected to generate a whopping 21% Increase IN CORPORATE PROFITS**

—Forbes

GREAT BAY

[1] https://www.forbes.com/sites/insights-hitachi/2017/12/18/5-areas-where-the-iot-is-having-the-most-business-impact/#1820e28f4396

[2] https://www.forbes.com/sites/insights-hitachi/2017/12/18/5-areas-where-the-iot-is-having-the-most-business-impact/#1820e28f4396

Early adopting organizations have already begun to see IoT investments pay off. In fact, Amazon's use of IoT-enabled robots at fulfilment centers have cut operating expenses by 20%, saving $11 million dollars per year—with an estimated savings of more than $5 billion per year if implemented globally.[3] Similarly, Harley-Davidson's implementation of smart manufacturing principles in one of its facilities has improved net margin by 19%, reduced costs by 7% and increased productivity by 2.4%.[4]

With results like these, it's clear there's value in IoT adoption. Businesses with well-defined IoT use cases, like Amazon and Harley-Davidson, will be the first to reap the benefits. But in this game of rewards, there are still plenty of risks that require mitigation through careful planning, cross-functional teamwork and mature security measures.

MORE DEVICES, MORE PROBLEMS

Most organizations already have a variety of IoT devices connected to their networks. Examples include VoIP phones, printers and surveillance cameras. The current challenge is how to support and secure the next wave of unmanaged endpoints, like medical devices, thermostats, sensors, smart light bulbs, industrial controllers, smart appliances or any of the thousands of other connected device types. Ready or not, the next generation of connected devices is coming—fast. Analysts predict IoT technology will be built into 95% of new product designs by 2020[5], resulting in more than three times more IoT devices than laptops, tablets and smartphones.[6]

BY 2020,
more than 25% of
IDENTIFIED ATTACKS
in enterprises
will involve IoT

With this influx of connected devices within an organization, IoT introduces new challenges for IT and Security. For some businesses, operational IoT challenges can hinder implementation, adoption and return on investment. Additionally, IoT increases an organization's attack surface, making network security and data protection far more complex. Large numbers of devices—many not associated with a user and not managed by IT—are connecting to a variety of networks and sending data to a variety of destinations.

Among more than 5,000 enterprises surveyed, just 10 percent of those who have implemented or will be implementing IoT feel confident about their ability to secure those devices.[7] There are multiple reasons for this. One is because IoT device discovery is difficult for security and network teams. There are many devices on the network whose identity are unknown to the organization. Another reason is the extreme vulnerability of the devices themselves since most have not been built with proper security hardening. For example, 80% of tested IoT devices failed to require passwords of sufficient complexity and length, and 70% did not encrypt communications to the internet.[8]

Additionally, there's a disconnect between IoT risks and the priority IoT security receives within an organization. Analysts predict that more than 25% of identified attacks in enterprises will involve IoT by 2020, but IoT accounts for only 20% of IT security budgets.[9] Thus, organizations that intend to reap the full rewards of IoT adoption will need to have people, process and technology in place to secure the IoT attack surface.

BY 2020 NEW
IoT TECHNOLOGY
will be built into 95%
of new product designs

[4] http://www.digitalistmag.com/digital-supply-networks/2016/07/18/how-harley-davidson-and-other-companies-deliver-individualized-products-04331406
[5] Gartner, "Top Strategic Predictions for 2018 and Beyond: Pace Yourself, for Sanity's Sake", September 29, 2017
[6] Gartner, "Beyond BYOD to IoT, Your Enterprise Access Policy Must Change", August 26, 2016
[7] AT&T's 2017 Global State of Cybersecurity Survey
[8] Internet of Things Research Study, HP, 2015
[9] IDC Worldwide Security Predictions, 2016

IoT RISKS IN ACTION

IoT risks aren't theoretical; they are being experienced by organizations today. Among 3,100 companies surveyed globally, 84 percent of those who have implemented IoT have already experienced a security breach as a result.[10]

Vulnerabilities that would allow cybercriminals to gain control of IoT devices have already been identified in endpoints such as cameras, cardiac devices, baby heart monitors and webcams. Recently, there has been a sharp increase in Distributed Denial of Service (DDoS) attacks using IoT devices. The increase is largely due to the rise of for-hire DDoS services and the lack of security found on many IoT devices, which have made the attacks accessible and within reach of many hackers. And as the number of IoT devices continues to surge with no sign of improved secure configurations, it is doubtful these attacks will subside.

What methods are hackers using to compromise IoT devices? Most attacks are carried out through one of the following methods:[11]

Code modification

Attackers inject or modify code that is running or stored on the device.

Key compromise

Attackers gain access to the encryption key and use it to unencrypt and access data.

Password-based vulnerabilities

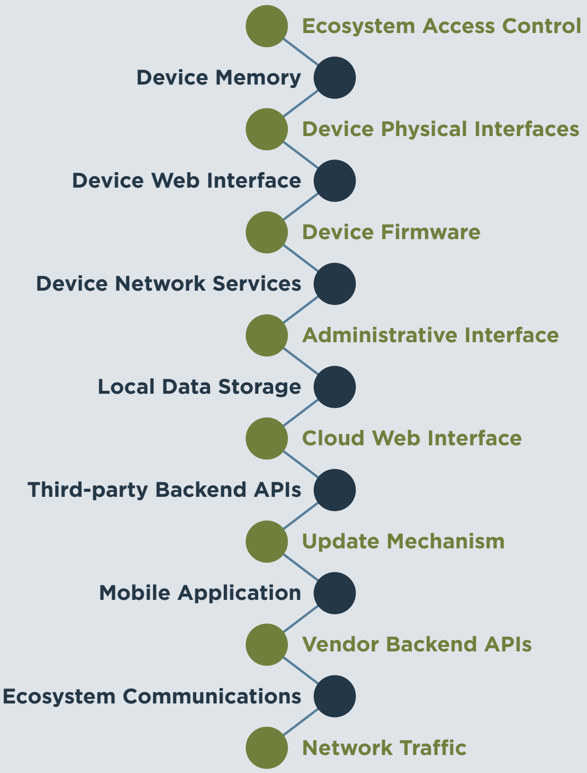
Attackers steal or crack a password to access the network.

Man-in-the-middle

Attackers relay, alter or intercept a communication between two devices or parties.

Understanding the IoT Attack Surface[14]

Regardless of the attack method, organizations have labeled IoT devices as the second most common source of a data breach in the last year—just behind employee mobile devices.[12] The business effect of those successful data breaches ranges from operational impact, downtime, reputational damage and loss of customers and their trust—all of which, ultimately, lead to lost revenue.[13] The following 15 IoT attack surface areas, each with their own respective vulnerabilities, have been identified by Open Web Application Security Project (OWASP), a non-profit charitable organization focused on improving the security of software. This list provides organizations with a starting point to identify and ultimately address IoT vulnerabilities.



IoT Attack Surface Areas

The work OWASP has done to outline IoT attack surfaces demonstrates just how vulnerable IoT devices are to attack and misuse. Without careful risk mitigation, this increased attack surface opens businesses up to dozens of new blind spots. Organizations looking to reap IoT benefits must perform detailed risk assessments of their current security posture, and make a plan to improve security maturity.

[10] Aruba Networks — The Internet of Things: Today & Tomorrow, 2017
[11] https://www.networkworld.com/article/3202767/internet-of-things/the-fight-to-defend-the-internet-of-things.html
[12] AT&T's 2017 Global State of Cybersecurity Survey
[13] AT&T's 2017 Global State of Cybersecurity Survey
[14] https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

THE STARTING POINT FOR IOT SECURITY

Three critical components to secure IoT deployments:

secure & scalable network

physical & digital security

device identity awareness

Although 90% of organizations have conducted enterprise-wide cyber risk assessments in the past year, only 50% have conducted risk assessments specific to IoT threats.[15] To protect the expected 21% profit increase generated by IoT, it is critical organizations rally around IoT security by giving it the strategic planning, manpower and monetary commitment it requires.

Specifically, experts have identified three critical components to securing IoT deployments: a secure and scalable network, physical and digital security, and an understanding of device identity[16] First, with more devices joining the network than ever before, the scalability of a network is more critical than ever. Organizations will need to carefully design their network and revisit their network segmentation strategy to securely support IoT. Secondly, the data accessed, created and communicated by IoT devices must be secured both in-transit and at rest in order to meet compliance regulations or protect business advantage. Organizations will need to identify the use case for every type of IoT device, as well as determine the confidentiality and protection requirements of all data being stored or transported. Finally—and perhaps most importantly—is the issue of device identity. In order for IoT deployments to be successful, devices must be known and trusted. Without this, they should not be allowed to connect to the corporate network. Unfortunately, this process is more difficult for IoT devices than it is for traditional endpoints. It is paramount that IT and Security teams have a way to identify every device that connects to the network and can assess if the device is "telling the truth" about its identity at each and every moment of its connection.

There is no question IoT introduces new security complexity for organizations, but it is not without its rewards. Security teams who prioritize careful planning and full visibility into all devices on the network will protect the payoff of IoT—allowing their organizations to surpass the competition in both innovation and efficiency.

[15] AT&T's 2017 Global State of Cybersecurity Survey
[16] https://www.helpnetsecurity.com/2017/12/18/cio-tips-iot/

GREAT BAY

8500 Normandale Lake Blvd • Minneapolis, MN 55437
+1.763.251.1400 • GreatBaySoftware.com