eBook

5 of the Scariest Things About the Internet of Things

Many IoT devices still pose major security issues that can cost us everything

CALIAN®

www.calian.com

1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

From Wi-Fi–enabled LED bulbs, to thermostats, sensors and more, the internet of things (IoT) is fast becoming embedded in everyday life.

At its most basic, the “things” in IoT are simply devices (consumer or commercial) that have embedded chips that enable the device to receive and communicate data. It is this ability that gives them tremendous power to save us time and add considerable convenience to our over-scheduled and hectic lifestyles. But, as the saying goes, with great power comes great responsibility.

Unfortunately, responsibility seems to have taken a back seat to profit. And there’s definitely a lot of profit to go around: according to Verified Market Research, a global research and consulting firm, the IoT market was valued at US$212 billion in 2018 and is expected to grow to a whopping US$1.3 trillion by 2026.

That increase in value is being driven by exponential growth, both in the number of devices and the number of apps; however, the strong security measures made necessary by this technology are lagging well behind.

CISOMAG, a magazine for chief information security officers, reported on some examples of the risks associated with IoT devices:

- After several months of research, Chinese researchers successfully broke into the Amazon Echo by using multiple vulnerabilities in the Echo system to achieve remote eavesdropping, which they demonstrated live at a DEFCON security conference in 2018. (They notified Amazon beforehand, which quickly pushed out a security patch.)
- Not long ago, security giant Avast sounded the alarm about smart coffee machines, the kind that owners can control via their phones or smart speakers like Amazon’s Alexa. According to a spokesperson, this creates a network vulnerability that is difficult to overcome. “Coffee machines are not designed for security,” he said.
- Academic researchers from England and Sweden designed malware that can use the microphone on your smartphone to steal passwords and codes.
- One of the most high-profile cases involved Ring, an Amazon-owned company that sells home security products. In a class action suit filed in late 2019, the plaintiffs allege that “[Ring’s] lax security standards and protocols render its camera systems vulnerable to cyberattack,” making users unsafe in their own homes and causing significant harm.
- The FBI has stated that smart TVs have a number of security issues that make them vulnerable to different kinds of threats.

Clearly, IoT security risks are both widespread and diverse. Here, then, are five noteworthy dangers associated with internet-connected devices.

1

Lack of security standards

These days, when you look at the IoT manufacturing industry, it's pretty much the Wild West out there. The fact is, many IoT devices are simply not designed with security as a priority. *Harvard Business Review* reported on a study that found an astonishing 80% of manufacturers do not routinely test their IoT apps for security vulnerabilities. Part of the problem is they aren't being forced to: slow-moving governments simply can't write new regulations fast enough to keep pace with the rapid evolution in IoT technology.

In the US, there are multiple overlapping federal and state agencies (plus international ones, as well) claiming some jurisdiction. This results in a confusing array of regulations, leaving companies unsure of their responsibilities and giving hackers a green light to keep doing what they do.

As HBR points out, manufacturers can't afford to wait for regulators to catch up: security and privacy need to be an integral part of the design and development process. Part of the problem is that security testing tends to occur during production, when it is too late to make major changes. For example, consider the issue of default user names and passwords, which consumers often don't change. A simple solution is to create apps that force users to set up new credentials before the device can be used. Another is to make sure devices can receive security updates throughout their lifespan to ensure they remain as secure as possible, regardless of the new tricks that criminals come up with in future.

Without a concerted effort, manufacturers will continue putting their customers at risk and leaving themselves open to the potential for lengthy and expensive litigation.

2

User complacency

When it comes to internet security, the knowledge of the average user is generally limited. End users need to educate themselves on the potential dangers of IoT devices and how they can affect their personal and business lives. (Many IoT devices are continually introduced into the corporate environment, posing a threat through potential holes in cybersecurity.) Both IT and facilities departments need to create more comprehensive policies and procedures, lists of approved device types, and more, and need to enhance device monitoring to thwart potential threats.

Today, companies like Microsoft and Apple embed relatively strong security measures into their computers and smartphones automatically (after many years of trial and error), so users may have a false sense of security, assuming that all internet-connected devices are equally protected against malicious actors.

But, as we know, IoT technology is very, very new. Just as the early PCs had numerous vulnerabilities, security protocols for smart devices are still in their infancy.

Forbes offers this advice to business and consumer IoT users:

- When choosing a device, go with a well-known brand. While this is no guarantee of safety, reputable manufacturers care about their name, so it is in their interests to protect you and their brand.
- Carefully read and follow the device's security instructions. It's likely the developers have spent at least some time working to minimize potential risks, so following their instructions just makes sense.
- Never use default passwords. Create a separate, strong password for each of your IoT devices as soon as you start using it.
- Keep your software up to date. New security holes get identified all the time, requiring developers to patch them and send out new software to users. Failing to implement these updates could lea

3

Malicious botnets

Cybersecurity company Norton defines a botnet as “a string of connected computers coordinated together to perform a task.” Botnets began, innocently enough, as a way to enable group discussion in chat rooms. But illegal and malicious botnets soon followed.

The Internet of Things Security Foundation, a non-profit organization aimed at tackling IoT security challenges, sees IoT botnets as the cybersecurity industry’s next big worry.

A malicious botnet is one that is infected with malware that enables the cybercriminal to remotely control the devices without the owner’s consent or knowledge. Malicious botnets are most commonly used to stage distributed denial of service (DDoS) attacks that overwhelm a website or online service with more traffic than can be accommodated, rendering the target inoperable.

For example, in late 2016, a large swath of the internet stopped working due to the Mirai botnet, which targeted Dyn, a company that controls much of the internet’s domain name system (DNS) infrastructure. The DDoS assault brought down numerous sites in the US and Europe, including Netflix, Reddit, Github, CNN, The Guardian, and Twitter. And last year, a new Mirai strain was identified that specifically targeted enterprise-class IoT devices.

In addition to websites, a botnet can wreak havoc on a large scale and has the potential to knock out major infrastructure, such as transportation systems and electricity grids.

4

Counterfeit IoT devices

Forbes' recommendation, that it's best to go with a well-known brand when choosing an IoT device, is based on the assumption that trusted brands will have better security. But another good reason to stick with big names is that it reduces the risks of accidentally buying a counterfeit IoT device, also known as a copycat.

Counterfeits can be difficult to spot. They often look the same as the original, right down to a (fake) manufacturer logo, which is why it is so important to only buy from trusted vendors. Counterfeits have widely infiltrated sites such as Amazon, eBay, and others. Purchasers need to remember that online marketplaces are platforms, not vendors—it's the actual seller that is key. To reduce copycats, some manufacturers have established online verification processes that allow users to confirm device authenticity.

In addition to inadequate security, malicious counterfeits can be designed to intercept or send data without the user's knowledge. The risks associated with counterfeits are high and can include everything from simple data theft to a ransomware attack, to destruction of critical systems.

Enterprises need to be especially vigilant to ensure that employees cannot add internet-connected devices without the knowledge of the IT department. This is easier said than done: in 2018, 802 Secure, which develops IoT signal-intelligent technology, examined cloud threat intelligence from a group of large enterprises (more than 10,000 employees) and found that 90% of these organizations had undetected wireless networks separate from their official infrastructure, and 100% of the companies contained "rogue" (non-sanctioned) IoT devices transmitting data to other individuals, networks and the cloud.

5

Loss of data integrity

IoT devices are all about data: generating it, sending it, receiving it. When this data is not encrypted, it can be intercepted. This goes beyond the obvious (and very real) risks associated with the possible theft of high-value data like passwords and banking information. For example, imagine what could happen if an internet-connected medical device were to send inaccurate information to healthcare providers, or stop sending it altogether.

This concept is more than a potential plot for a Hollywood movie. In 2017, the US Food and Drug Administration reported that an implantable cardiac device developed by St. Jude Medical had serious vulnerabilities that, if exploited by a hacker, could administer incorrect pacing or shocks or deplete the battery, effectively killing the device (and, possibly, the user).

In one report, network security firm Zscaler documented its examination of 56 million IoT device transactions from 1,051 enterprise networks over the course of a month. Zscaler found that more than 40% of these enterprises did not encrypt their traffic, thus exposing them to what is known as man-in-the-middle attacks. In this type of attack, hackers put themselves in a position to steal or manipulate corporate data.

The vulnerable devices that were generating all of this data included a huge range of internet-connected hardware, such as cameras, smart printers, smart TVs, IP phones, smartwatches, networking devices, and data collection terminals. (Data collection terminals were the biggest data producers, generating more than 80% of outbound data transactions.) Significantly, of all the millions of data transactions examined, more than 90% were unencrypted.

The Solution

Identify risks and secure devices

Beyond discovering the assets, a monitoring platform can identify the risks and vulnerabilities for devices in the office and at remote locations, as well as those interacting with cloud environments.

A monitoring platform determines what a device is and how it is being used and correlates that information against the platform's inherent understanding of device characteristics and behaviors. It then compares a device's individual risk profile with the organization's risk posture to provide automated security and policy enforcement.

Automate and enforce security policies

If a monitoring platform identifies a vulnerability, risk, or security gap, it can automate security and policy enforcement. It can then orchestrate the necessary actions, in conjunction with IT or security management solutions, or at the network level. This includes actions like feeding device risk data to a security information and event management (SIEM) database or configuration management database (CMDB), triggering a vulnerability scan, if appropriate, and kicking off a process to install software or block or quarantine a device.

Conclusion

As long as the number of IoT devices entering homes and businesses continue to rise—together with the ever-increasing resourcefulness of cybercriminals—it's safe to say that security issues will continue to plague the industry.

The IoT sector needs better manufacturing and security standards, clearer and more comprehensive regulations, and more effective counterfeit detection and law enforcement. It also needs to make robust data encryption the norm—not the exception.

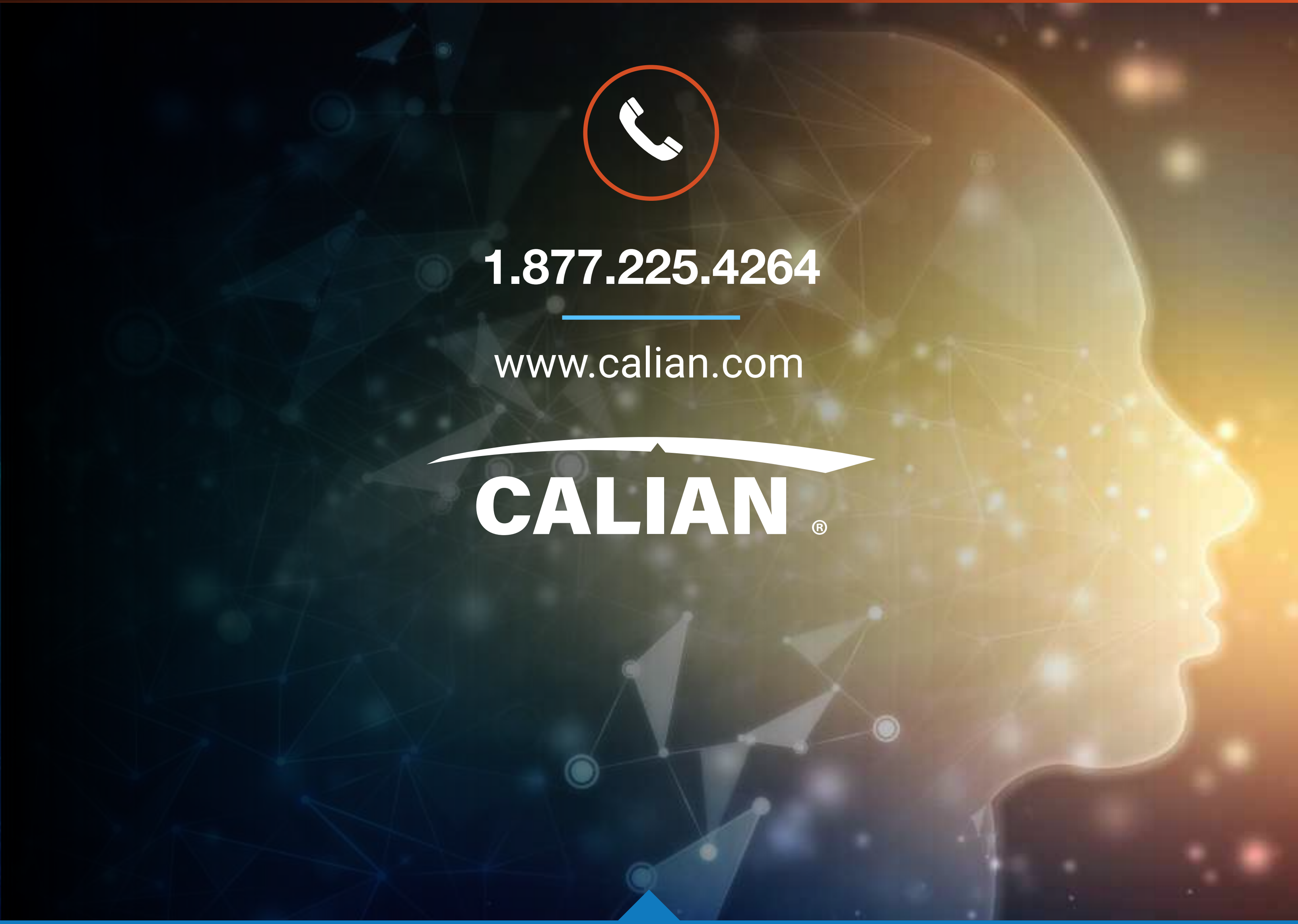
Most importantly, users, both individuals and businesses, need to understand that just because a device does something innocuous—makes coffee, prints documents, tells you how many steps you took today—doesn't mean it's harmless.

IoT devices have the potential to make our lives much easier. But they also have the potential to cause real harm, to our businesses, our pocketbook—even our health—which is why each of us needs to start valuing security as much as we value convenience.

CALIAN®

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

Contact us for a free consultation or to receive a free Cloud Security Audit to assess the effectiveness of your current cyber security initiatives.



☎

1.877.225.4264

www.calian.com

CALIAN ®

References

802 Secure. (2018, May 16). *802 Secure shares IoT threat research at Internet of Things World.* Cision PR Newswire. Retrieved from https://www.prnewswire.com/news-releases/802-secure-shares-iot-threat-research-at-internet-of-things-world-2018-santa-clara-300649218.html

CISOMAG. (2019, May 22). *Over 90% of data transactions on IoT devices are unencrypted.* Retrieved from https://www.csoonline.com/article/3397044/over-90-of-data-transactions-on-iot-devices-are-unencrypted.html

CISOMAG. (2020, January 10). *10 IoT security incidents that make you feel less secure.* Retrieved from https://cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure/

Dickerson, B. (2016, July 12). *IoT botnets might be the cybersecurity industry's next big worry.* TechTalks. Retrieved from https://bdtechtalks.com/2016/07/12/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/

Franceschi-Bicchierai, L. (2016, September 29). *How 1.5 million connected cameras were hijacked to make an unprecedented botnet.* Vice. Retrieved from https://www.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

Kontsevoi, B. (2020, March 31). *IoT Threats And What To Do About Them.* Forbes Technology Council. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2020/03/31/iot-threats-and-what-to-do-about-them

Norton. (n.d.). *Malware 101: What is a botnet?* Retrieved August 21, 2020, from: https://ca.norton.com/internetsecurity-malware-what-is-a-botnet.html

Pankov, N. (2019, March 19). *Mirai goes enterprise.* Kaspersky. Retrieved August 21, 2020, from https://www.kaspersky.com/blog/mirai-enterprise/26032/

Tannenbaum, A. (2017, April 27). Why do IoT companies keep building devices with huge security flaws? *Harvard Business Review.* Retrieved from https://hbr.org/2017/04/why-do-iot-companies-keep-building-devices-with-huge-security-flaws

Valerio, P. (2018, April 16). *Copycats pose a serious security threat to the IoT.* IoT Times. Retrieved from https://iot.eetimes.com/copycats-pose-a-serious-security-threat-to-the-iot/

Verified Market Research. (2020, July 14). *Internet of Things (IoT) market worth $1319.08 billion, globally, by 2026 at 25.68% CAGR: Verified Market Research.* Cision PR Newswire. Retrieved from https://www.prnewswire.com/news-releases/internet-of-things-iot-market-worth-1319-08-billion-globally-by-2026-at-25-68-cagr-verified-market-research-301092982.html

CALIAN®