IoT security: It is about context and correlation

Trying to defend against every IoT device in the company might not be the answer but having rules in place could help. One of the biggest threats is shadow IT. Evan Schuman reports.

The internet of things (IoT) is ill-defined and often unseen by security and IT teams, representing what Ernst & Young (EY) Managing Director Douglas Clifton sees as "the single largest addition to the enterprise attack surface." Shadow IT headaches make IoT far more dangerous and insidious and IoT on the cloud can often make a very difficult situation nearly impossible.

Today's COVID-related massive corporate telecommuting explosion is forcing enterprise CISOs to deal with consumer-level, home-based IoT security problems and how those IoT-based refrigerators, doorbells, IP cameras and Amazon Echos ("Alexa, download all of my employer's payroll records") now directly threaten the most sensitive corporate intellectual property.

Arguably the biggest single security problem with IoT is that, with relatively few exceptions in enterprises of more than $3 billion in annual revenue, companies are trusting the manufacturers of these devices to engage in enterprise-level security procedures — something that very few IoT manufacturers can or are inclined to try to do. The challenge with many consumer and business-class IoT devices is their inability to layer on security software or to update firmware.

Practical IoT

Let us start with a practical definition of IoT. Many define it as any device that connects to an IP network, but some antennae-based devices have independent communications capabilities, often via satellites. Clifton, who also serves as EY's industrial cybersecurity and IoT lead, says that his favorite IoT definition is "an IT-connected device that is outside of the IT umbrella management, so not a server or laptop." That could include radio frequency identification (RFID) tags attached to pallets on long-distance ships or a restaurant grill that has a sensor tracking temperature and maintenance adherence.

The sheer scope of IoT in the typical enterprise today, coupled with how many are typically outside of asset management view, is one reason the IoT security problem is so difficult to master. In enterprise security and IT departments, even in corporations with strict departmental separations, IoT devices tend to involve both IT and security considerations. The executives typically are aware of less than 10 percent of existing IoT devices, says Scott Russ, security architect at the Nerdery consulting firm.

Much of that is because some shadow IT (such as facilities buying IoT door locks without vetting the products through the IT security team or maintenance doing the same with IoT lightbulbs) items have morphed

OUR EXPERTS: IoT

Kelly Albrink, senior security consultant, Bishop Fox
Douglas Clifton, managing director, Ernst & Young
Chetan Conikee, CTO, ShiftLeft
Frank Ford, partner and head of the global cybersecurity practice, Bain & Company
Scott Russ, security architect, Nerdery
David Shrier, program director and associate fellow, University of Oxford
Brian Tant, chief technology officer, Raxis
Evan Wolff, partner, Crowell & Moring

IoT

79.4ZB

By 2025 an estimated data volume of 79.4 zettabytes will be attributed to connected IoT devices

– Statista

into being IoT-equipped so slowly that IT and security do not think of them as IoT but rather as commodity facilities devices and, of course, the IoT devices planted by criminals.

This brings us back to the awkward definitions of IoT. For example, is every mobile device that an employee brings into the building (smartphones, watches, Airpods, games and the like) considered IoT? What about the IT-connected cars parked in the garage or the nearby parking lot? Many of them have tremendous capabilities to intercept, exfiltrate and send massive amounts of data.

Kelly Albrink, senior security consultant, Bishop Fox

"IoT is a buzzword that is sort of nebulous," Russ says. "There is not going to be one hammer that solves all IoT problems."

One approach Russ suggests is to not even try and get control of all of the existing IoT devices — you would fail anyway, he reckons — but to setup strict rules about any devices that are newly installed, requiring stringent security testing of each item. Then, in theory, as the existing IoT devices age out and die, the percentage of IoT control would go up until all known devices are covered by strict security. Shadow IT is a different issue.

Much of those requirements will have to be imposed on IoT device manufacturers, Russ says. "We'll purchase these widgets, but they must be fixed within a year or there will be consequences," Russ says.

What is the big problem some consultants have with that approach? Simply put, they don't trust the IoT manufacturers. And if the manufacturers are not behaving properly from a security perspective — a big if indeed — then imposing strict rules on them for action a year from now might be futile and ineffective.

"The manufacturers are the ones that are cutting corners," says Kelly Albrink, senior security analyst at Bishop Fox, a security consulting firm in San Francisco. "If I reverse engineer the (IoT) lightbulb, I will find the default encryption key. If you can exploit one, you can exploit all of them."

Still, Albrink conceded that enterprise security executives have little choice but ultimately to hope that the vendors take security more seriously. "At the end of the day, they still need a solution to their problems, so they end up trusting manufacturers whether they want to or not. Ask your vendors: 'When was the last you did a security assessment by a third party?'"

Limiting vulnerabilities

Albrink also suggested trying to mitigate the security problems by simply limiting where you permit IoT devices. "Don't use any type of electronic door locks in your sensitive areas. Limit to areas where you can afford to take risks. You may have an electronic door lock on your building's front door but don't use it on your server room."

> "If I reverse engineer the (IoT) lightbulb, I will find the default encryption key. If you can exploit one, you can exploit all of them."
>
> *– Kelly Albrink, senior security consultant, Bishop Fox*

Among Albrink's other top concerns: "The security of newer and still somewhat obscure wireless protocols including ZigBee, Z Wave and LoRaWAN (low power wide area network). The exposed debugging headers is

85%

Percentage of security network pros who say network security is more difficult than it was 2 years ago

– ESG

a pretty common finding that they exploit in hardware hacking projects, but it's extremely common and sometimes necessary in the hardware building process."

Chetan Conikee, founder and CTO of ShiftLeft, a security application testing firm in Santa Clara, Calif., recommends that CISOs audit "IoT vendors' software development practices, including asking to see pen-test results and asking if your teams can run their own pen-tests. If the internal resources exist, this could include auditing source code as well. If an IoT vendor doesn't have a public bug bounty program, that isn't necessarily a bad thing. However, if they won't share details on their AppSec policies/procedures, it's reasonable to question how seriously they take security," he says.

Scott Russ, security architect, Nerdery

"Assume IoT devices are the weakest link in the security chain. This includes tightly monitoring privileged access with strong user management policies, authentication with MFA (multifactor authentication), strong passwords, etc. and understanding what data and systems IoT devices can access if compromised, and minimize that access in advance," Conikee says.

Nerdery's Russ encourages CISOs to push for greater network access control ("I know all about those routers shoved under people's desks," he quips), although he acknowledges that IoT devices with independent antennae "would be immune."

Much of Russ's most serious concerns involve the rushed corporate telecommuting arrangements. "The smart refrigerator: Who knows what it's doing? We can't control home networks, but we can control the devices that users use to connect to corporate environments. First, you cannot allow split tunneling. It really all depends on how draconian you want to be," he notes.

Legacy devices

Another Russ apprehension: Some of these IoT devices are many decades old and long predate how today's security teams define IoT. As a result, those devices might not be on the security team's radar.

"Oftentimes, IoT devices are an integral part of a business process that was around long before the company had any formal security department," Russ says. "These business processes are grandfathered in and CISOs are hesitant to enforce security standards out of fear of breaking a critical revenue-generating business process."

In many scenarios, "the legacy process and its IoT devices are simply ignored," he continues. "They are granted a security exception and allowed to continue to operate outside of the guardrails placed on other devices on the network."

So, what should security do about these legacy IoT devices, as well as any new ones?

> "Assume IoT devices are the weakest link in the security chain."
>
> – Chetan Conikee, CTO, ShiftLeft

"CISOs should force every device to authenticate to the network," Russ says. "Technologies like network access control (NAC) can ensure that devices meet requirements before being allowed to communicate on the network. NAC device policy can be used as a guide during IoT vendor selection. If an IoT device doesn't meet the requirement, eliminate that vendor from the conversation and find one who does."

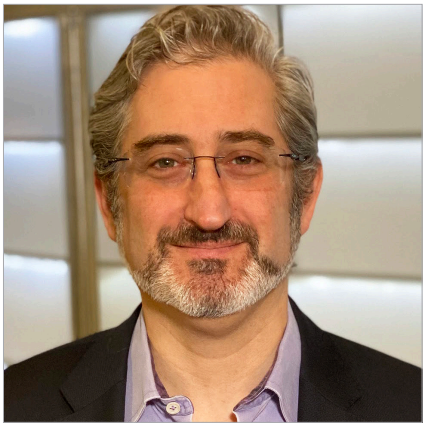
Exceptions, though, "can be made if there

$1.1T

Estimated size of the IoT market in 2026

– Fortune Business

is a critical business need that supersedes the security risk, but it should not be the CISO's job to solely make that decision," he notes. "The CISO should communicate the risk to the rest of the executive team, document the decision with a risk management program, and revisit it every year to determine if it can be resolved."



David Shrier, program director and associate fellow, University of Oxford

But, Russ stresses, NAC can often be a tad overaggressive, blocking communications that it should not block (false negatives). "One mistaken authentication and you can wipe out your whole call center," Russ says, adding that a more moderate approach might be preferable. For example, the NAC could merely notify any devices that fail authentication but allow the communication to proceed. In other words, allow the unauthenticated communication device to stay on the network, however this process gives the security team time to remediate those devices or at least try.

> "It really all depends on how draconian you want to be."
>
> – *Scott Russ, security architect, Nerdery*

Personal IoT

David Shrier, a program director and associate fellow at the University of Oxford, points to two other IoT concerns: home-based devices that do more than they claim, especially with their cameras and microphones; and the mechanics of the device manufacturing.

Internet-connected televisions and digital personal assistants, among other consumer devices, are constantly listening for commands, meaning that ultra-sensitive business communications could be captured, recorded, transcribed and exfiltrated to wherever the IoT device chooses to send it. To state the obvious, just because an IoT device was originally programmed to communicate with its mothership — its manufacturer, presumably for updates — that does not mean that a cyberthief, corporate espionage agent or state actor could not trick the device into sending the data to them.

Shrier says that a colleague did a scan recently and found 70 different listening devices in a home. Now that is some serious data leakage if, for example, an enterprise's senior executive is discussing hostile takeover details in front of them. Shrier's suggestion? "Have those conversations in a different room from where they have the [IoT] TV" or other listening devices. "Your home is a security nightmare," he says.

"One aspect of IoT security that often goes overlooked is the firmware on the devices themselves. Often the way hardware is purchased is that a company runs an RFP and takes the low bidder, who then assembles a device that has a 12-year-old unpatched version of Linux with numerous security holes," Shrier says. "The number of companies that have a comprehensive IoT security update and audit process is not as high as you would like. [Do] you know how to check for the firmware version of your microwave? You can't."

Then there is every security professional's favorite bogeyman: the cloud. As bad as on-premise IoT security visibility is — and that now includes a plethora of home office environments — at least you ostensibly have authority over those environments once you stumble upon the IoT device. That is often not the case in the cloud.

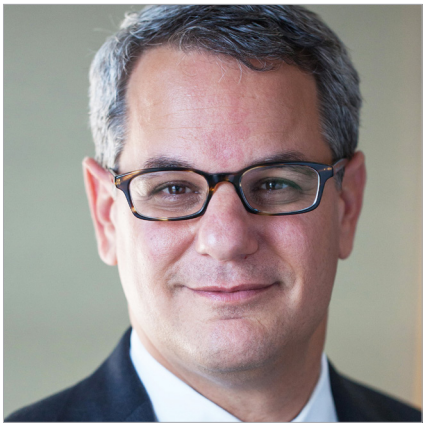
>30B

Estimated number of active IoT devices will surpass 30 billion in 2020

– DataProt

Even if an enterprise is using one of the megacloud vendors, which is quite likely, visibility into the IoT devices that platform is using is typically zilch. That is true even if those devices potentially could impact your hosted data's security.

Cloud vendors generally have some awareness of a small percentage of their own IoT devices, as they are subject to the same shadow IT and other IoT headaches as every other enterprise. That means that even if the cloud vendor suddenly embraced complete transparency with its corporate tenants — an action unlikely to occur — the CISO's visibility into the IoT situation in the cloud would still be, well, highly clouded.



Evan Wolff, partner, Crowell & Moring

By the (law) books

Beyond the pure security protection issues that CISOs need to obsess over are the legal and compliance/regulatory implications. Evan Wolff, a partner at the Washington, D.C.-based Crowell & Moring law firm, says an often overlooked area for CISOs on IoT is accurately and continually telling shareholders and regulators the realities of the enterprise's IoT security situation.

"This is more of a carbon than a silicon problem," Wolff says, meaning that it is a matter of getting humans to think more like an attorney. "They need to get their lawyers and business leaders and corporate executives much more aware and informed about what the true challenges are. This could be material in your SEC filings," Wolff says. "They need to think through how they draft and manage risk and they need a good incident response playbook."

Brian Tant, chief technology officer of the Atlanta-based penetration testing firm Raxis, adds another legal point, this one dealing with ownership of intellectual property and particularly data.

"Conventional wisdom says that the owner of a system also owns the data generated by that system. But increasingly, IoT devices come with licensing models that allow the vendor to claim ownership of data or metadata, take control of systems, or make changes to system configurations without notice," Tant says.

"This model doesn't always mesh with change control and auditing," he continues. "These devices that are being deployed into production are, quite literally, black boxes. Yes, they have functional specifications, but the inner workings often remain proprietary. Security standards are largely non-existent between vendors and the hardware is far from homogeneous."

Another perspective comes from Frank Ford, the head of the global cybersecurity practice and a partner at Boston-based Bain & Company, a management consulting firm.

> "They need to think through how they draft and manage risk and they need a good incident response playbook."
>
> – Evan Wolff, partner, Crowell & Moring

Ford, who is based in London, says that it is hard to overstate the security problems that come from an enterprise's typical deployment of IoT. When doing scans and network assessments, "these things just pop up in the environment," attributing much of it to shadow IT. That is met with security specialists "who are underfunded, running around checking their tails."

The easiest first step, Ford suggests, is to

83%

Percentage of companies that improved their efficiency by introducing IoT devices

– DataProt

sharply increase all data encryption efforts, on the hope that anything that an IoT device improperly exfiltrates might end up being worthless to bad guys. "You need to encrypt absolutely everything," Ford says. "The perimeter is expanded hugely by IoT."

Ford says that IoT devices with independent antennae "do pose a particular security threat," but at least the extra threat is only one-way. "Any device that has independent access can bring viruses back into the system, through your core firewalls, through your antivirus — but it needs network access to spread it. It can exfiltrate silently but not spread: That still needs the network."

> "You need to encrypt absolutely everything. "The perimeter is expanded hugely by IoT."
>
> *– Frank Ford, partner and head of the global cybersecurity practice, Bain & Company*

Attacking IoT security issues requires a two-pronged attack method. For all of the devices that are known — which could be a tiny minority of the IoT devices throughout the enterprise — there needs to be strict authentication of each device, any access to it from either direction and awareness and controls over what data it can access. For all the devices that are not known, there needs to be a robust effort to both deter shadow conduct as well as efforts to locate any and all unauthorized devices.

Albrink dubbed such efforts fox-hunting. "You need to try to locate every rogue wireless access point by walking around with directional antennas and finding things that don't belong. It requires specialized equipment" and "a ham radio nerd to do it."

Those approaches should address some of the corporate location issues. But attacking the IoT security problems when so much corporate work is being done in consumer environments is another issue. Does this mean that companies might need to require all corporate work be done in a room that is both free of IoT devices as well as shielded? Will the IoT security hunt force enterprises to insist on a return to Ethernet-only connections? Yes, IoT in the home is something that few CISOs intended to attack in 2020. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at (347) 480-1749, or via email at david.steifman@cyberriskalliance.com.

40%

Percentage of organizations that will look to secure IoT network traffic with traditional technologies to create "IoT segments"

– ESG