riskrecon

mastercard

Internet of Tip-offs (IoT)

A study of exposed IoT devices in the enterprise

14x

EDUs have a 14x higher rate of IoT device exposures

86%

of security findings affecting IoT devices are rated as critical

62%

Firms with exposed IoT have 62% higher density of overall security issues

Analysis conducted by

119 Cyentia INSTITUTE

Less than a decade after the establishment of the TCP/IP protocol,[1] enterprising engineers at Carnegie Mellon decided it was a good idea to give their local vending machine access to the Internet.[2] That first "thing" connected to the Internet started a slow burn that has turned into an absolute conflagration. Sometime in 2009 the "things" on the internet started to outnumber people, [3] and the future will include trillions of dollars in investment in IoT.[4]

IoT devices have made many facets of modern living easier (though we might question the value of an internet enabled toaster), but they have also increased the potential for attacks. Every connected device contains possible flawed software, and because many of these devices are connected to critical devices (in-home cameras and door locks), they represent an outsized potential for damage. Outside IoT specific attacks, insecure IoT devices can be co-opted for more traditional attacks such as the use of the Mirai botnet for distributed denial of service.

These problems are exacerbated because it seems like security for these devices is even more of an afterthought than it is in other software. Toss in an inability to easily patch vulnerable software and less than stellar long term support and it's obvious that any assessment of the security risk of an organization should contain an evaluation of IoT devices.

That's exactly what we do in this report, examine how IoT affects the risk surface of *organizations*. We italicize that to emphasize that this isn't a study of home-based devices, as is typical for IoT research. As we've done when examining up-to-date TLS deployment and unsafe services, we'll examine the prevalence of IoT devices within organizations, what types of devices we see, and how the presence of insecure IoT devices can correlate with other types of problems. We examine RiskRecon's dataset of millions of hosts controlled by more than 35k organizations.

> Thus, exposed enterprise IoT devices are a clear tip-off that other security issues exist across organization's infrastructure.

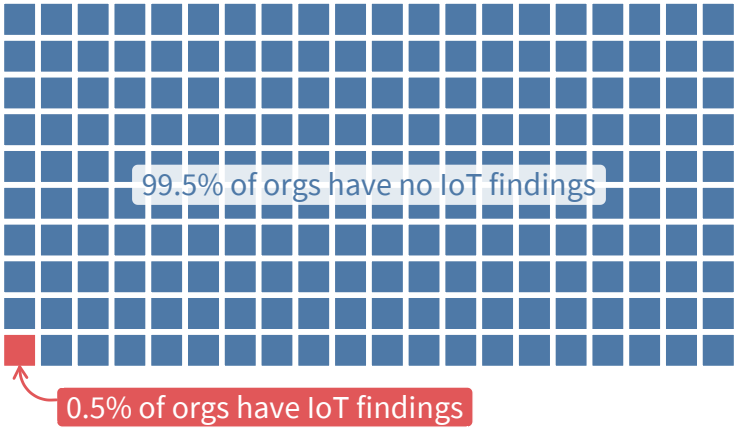
[1] TCP/IP RFC first published 1974, https://tools.ietf.org/html/rfc675.
[2] https://www.cs.cmu.edu/~coke/history_long.txt
[3] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[4] https://www.businessinsider.com/internet-of-things-report?IR=T

Prevalence of Exposed Enterprise IoT Devices

Despite 100s of millions of discoverable IoT devices on the Internet, we found a relatively small number of them among the external-facing enterprise assets in RiskRecon's dataset. Less than one twentieth of one percent (0.038%) of all scanned hosts owned by organizations are IoT devices. So, why the discrepancy? The answer is simple; RiskRecon takes care to ensure that hosts they assess belong to organizations rather than to individuals. We infer that the vast majority of discoverable IoT devices detailed in other reports are connected home devices.

There's a big difference between keeping individual hosts free of security issues and the organization being able to purge issues entirely from their infrastructure. This pattern manifests itself in Figure 1, with roughly 0.5% of organizations having at least one Internet-facing IoT device with detectable security findings. Still a blessedly low value, but not insignificant.

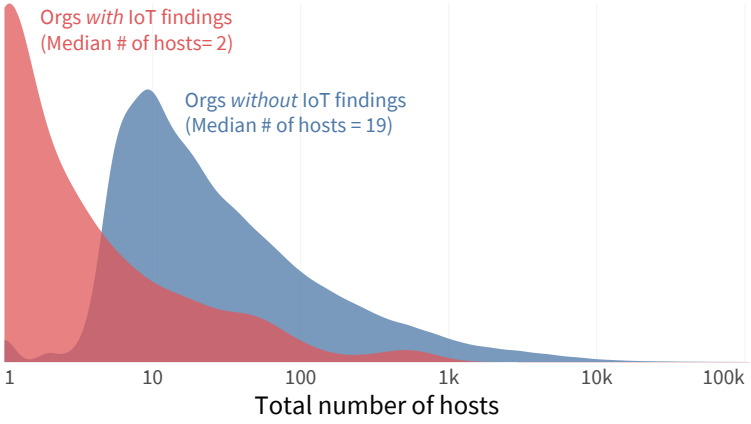
FIGURE 1: PROPORTION OF ORGANIZATIONS EXPOSING INSECURE IOT DEVICES



We discovered exposed IoT devices with security findings in less than 1% of organizations.

Of course, the rates of organizations with IoT findings are likely to vary based on a number of firmographic factors. And as you might expect, it's smaller organizations that tend to have more trouble keeping IoT devices from being exposed to the outside world. Below we see that organizations with exposed IoT devices typically have a small digital footprint (median of two Internet-facing hosts). Meanwhile, organizations that do NOT expose IoT devices have nearly 10x the number of hosts comprising their infrastructure and match the overall distribution we see for all organizations.

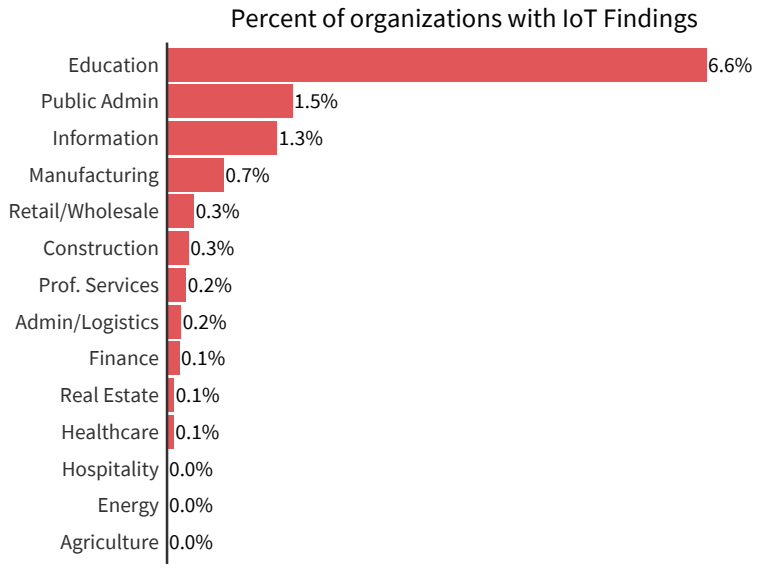
FIGURE 2: SIZE COMPARISON OF FIRMS WITH (RED) AND WITHOUT (BLUE) EXPOSED IOT DEVICES



Organizations with exposed IoT devices are more likely to have a smaller digital footprint.

Below we break down the percent of organizations with IoT findings by industry. Once again, we have to pity education, with a nearly 14x increase in likelihood of having IoT findings than the base rate of 0.5%. This is unsurprising given the positively byzantine networking environment of most educational institutions. We see a lot of variation across industries, though, with the top performers exhibiting a prevalence of IoT exposure that's well below the base rate of 0.48%.

FIGURE 3: COMPARISON OF IOT EXPOSURE RATES BY INDUSTRY



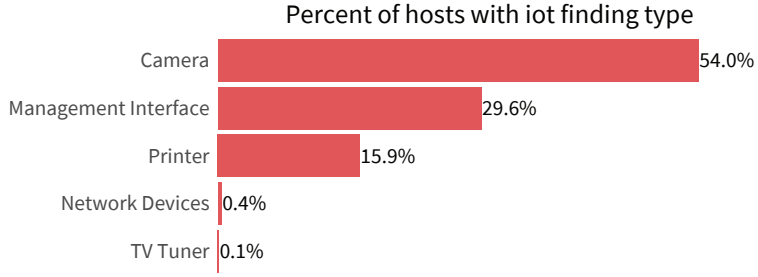
The Education sector has the highest rate of exposed IoT devices—nearly 14x the overall average across all industries.

Types of Exposed Enterprise IoT Devices

Knowing the prevalence of IoT devices and where they are most likely to be found is a start. But the next questions to ask are what types of devices they are and what can be determined about their level of security or insecurity. Afterall, it may be the intent to have the device accessible from anywhere, and it may be running secure software. Let's interrogate those possibilities.

First what types of devices are out there? In terms of the Internet-facing enterprise infrastructure assessed by RiskRecon, it's mostly cameras (54%), "management interfaces" (30%), and printers (16%). For that middle category of devices, the waters are a bit murky. These management interfaces are running generic IoT software such as the "Boa Web Server for IoT," but it's difficult to determine exactly what they are. In the case of the Boa example, it's basically a platform on which to build IoT device functionality but may not immediately reveal anything about the underlying device itself.

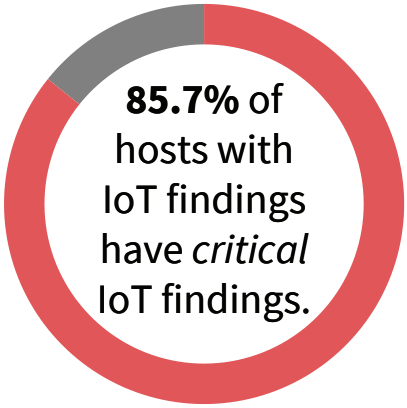
FIGURE 4: TYPES OF FINDINGS ASSOCIATED WITH EXPOSED IOT DEVICES



Cameras and printers are self-explanatory. The 'Management Interface' category consists of myriad devices using various development platforms.

IoT software is not exactly known for being a bastion of security, and we definitely find confirmation of that here. Nearly 86% of IoT devices have security findings rated as critical. To put that in perspective, only 2% of non-IoT hosts have critical findings. That means that the vast majority of IoT devices have flaws that are likely to result in serious compromise if exploited.

FIGURE 5: PROPORTION OF IOT DEVICES WITH CRITICAL SECURITY FINDINGS



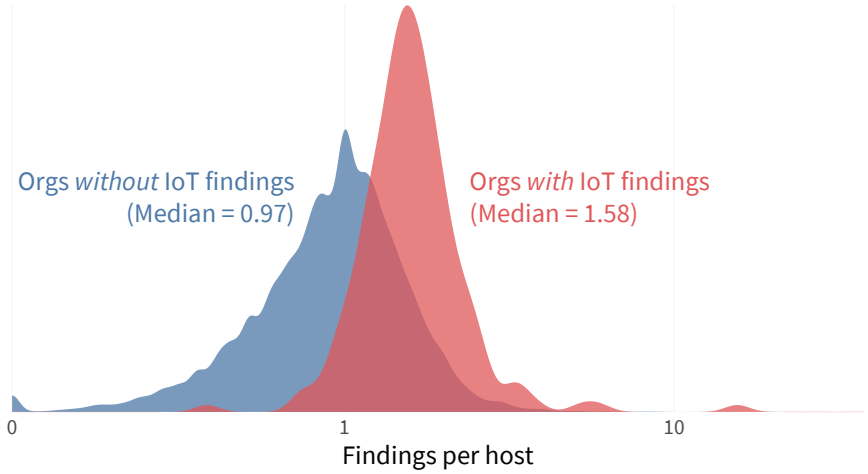
The vast majority of security issues affecting IoT devices are rated critical. Non-IoT devices have a critical finding rate of 2%.

Correlation of IoT Findings With Other Problems

As we've seen in several recent reports, the presence of one type of finding can be a harbinger of a wider range of security problems. This "where there's smoke, there's fire" principle is an important one for organizations looking to efficiently manage the overwhelming volume of issues clamoring for remedial attention. First, let's simply look at the density of findings, which measures the number of all security issues identified per host for each organization.

The figure below shows the density for organizations that have IoT devices and those that don't. The takeaway is that organizations with exposed IoT devices have 62% higher flaw density than those that don't. Thus, exposed enterprise IoT devices are a clear tip-off that other security issues exist across organization's infrastructure.

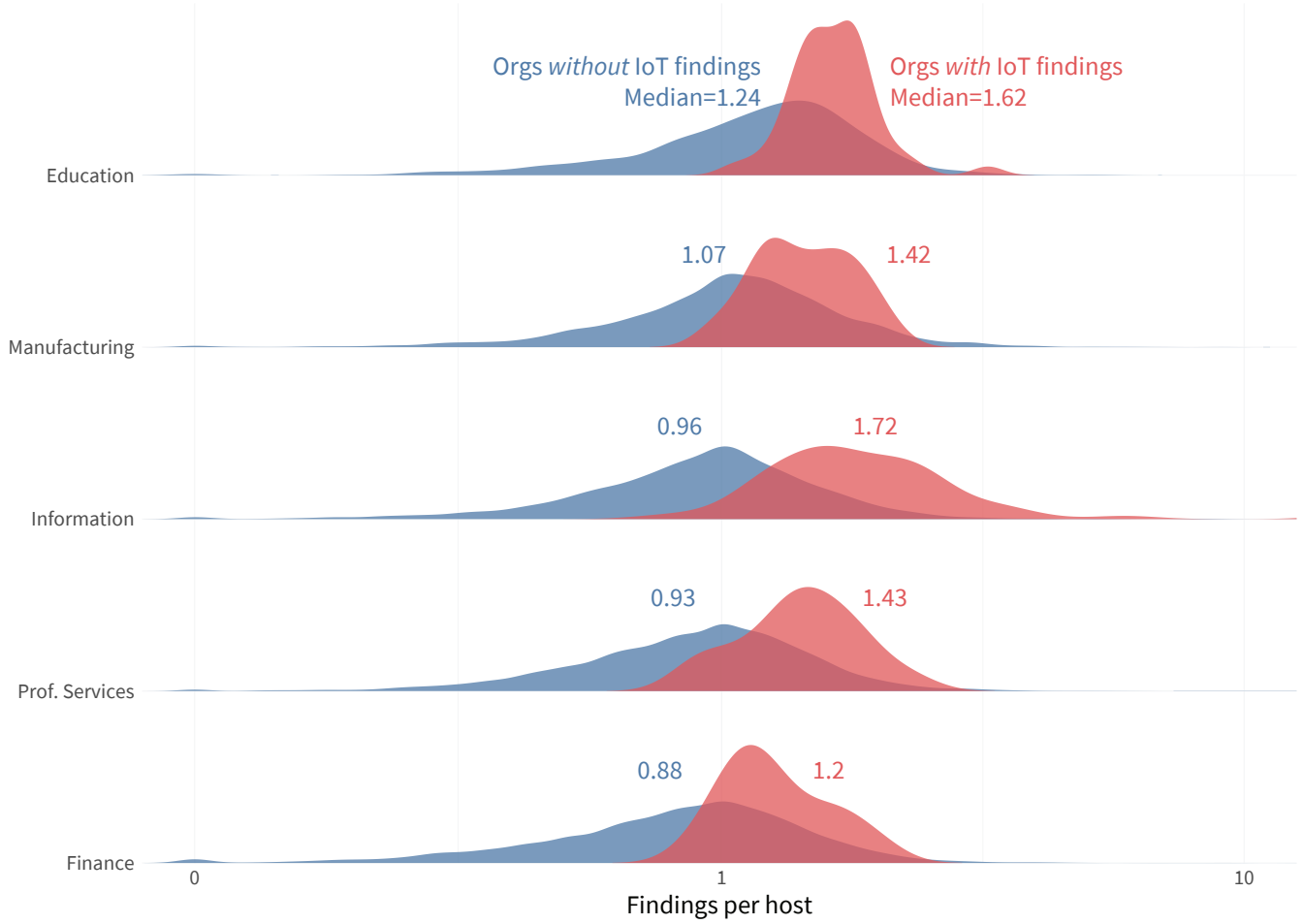
FIGURE 6: NUMBER OF SECURITY FINDINGS AMONG FIRMS WITH (RED) AND WITHOUT (BLUE) EXPOSED IOT DEVICES



Organizations with exposed IoT devices have 62% higher findings density than those that don't.

Furthermore, we find this 'IoT as a smoke signal' principle to be true across various industries. Again, Education leads the pack in finding density, but also shows a significant difference between institutions with and without exposed IoT devices. Interestingly, the Information sector has the biggest gap between the IoT haves and have-nots. Those with IoT devices exposed have nearly 80% higher median density of security findings. That suggests it's even more important to know what your partners in that sector (which includes providers of various types of IT services) are exposing to the internet.

FIGURE 7: FINDINGS DENSITY AMONG FIRMS WITH (RED) AND WITHOUT (BLUE) EXPOSED IOT DEVICES BY INDUSTRY

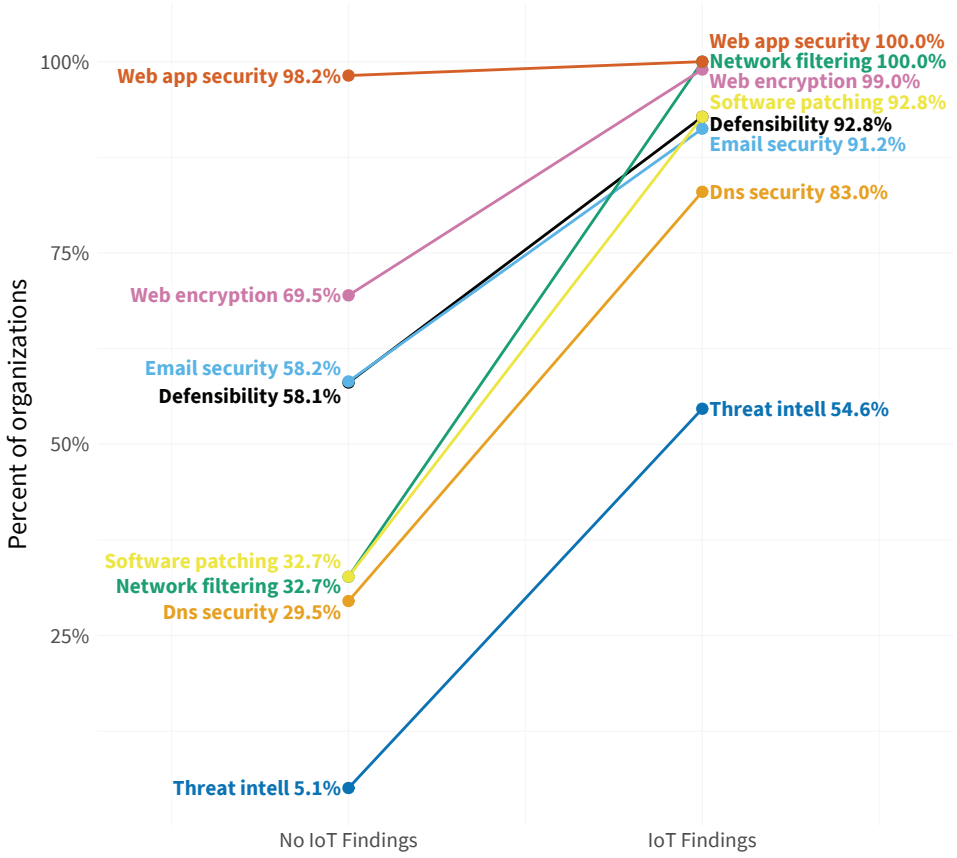


All industries show a higher rate of security findings among organizations that expose IoT devices to the internet. That seems particularly true for the Information sector, which includes IT service providers.

We now know that organizations with IoT devices exposed tend to also have a higher density of other security findings. But what types of findings are more likely for those organizations? Glad you asked.

In Figure 8, we see an increase across the board for all types of findings among firms that have exposed IoT devices. Issues associated with network filtering and software patching increase the most, but most categories jump 30% to 60% in prevalence. This also nearly guarantees (>90%) that firms will exhibit every type of finding other than those falling under DNS security or threat intelligence.

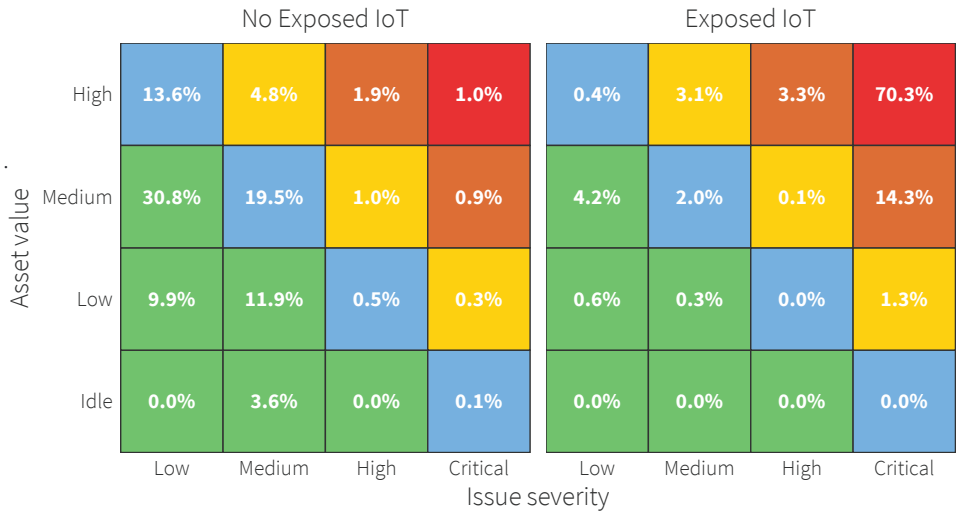
FIGURE 8: INCREASE IN TYPES OF SECURITY FINDINGS AMONG ORGANIZATIONS EXPOSING IOT DEVICES



Read Figure 8 like this: The proportion of firms with security findings related to web encryption is 69.5% among those that do NOT expose IoT devices to the internet. Among firms that DO expose IoT devices, that rate is 99%.

We'd be remiss if we didn't leave you with a view of how this looks through RiskRecon's risk priority matrices. As you can see, exposed IoT devices sit almost exclusively in the top right corner of the matrix where the dangerous combo of high-value assets and critical security findings collide.

FIGURE 9: RISK PRIORITY MATRICES FOR ORGANIZATIONS WITH (RIGHT) AND WITHOUT (LEFT) EXPOSED IOT DEVICES



Assets rated as high value support sensitive and/or critical functions. That's why the 70x jump in critical security issues among high-value assets exposing unsafe services is a major red flag.

How Can We Put This Into Practice?

Wondering how RiskRecon can help your organization take action on the findings from this report? Read this.

Enterprise Risk Management

RiskRecon's continuous IT profiling and security analytics give you intimate visibility into your Internet connected systems, where they're hosted, what their configuration is, and if it meets security requirements. RiskRecon's analytics discover the IT profile of every system and analyze each one against 41 security criteria like those examined in this report. Combined with RiskRecon's ability to automatically determine asset value at risk, your teams can easily identify issues, prioritize response, and act efficiently.

Third-Party Risk Management

Performing third-party assessments without objective data puts you at a huge disadvantage, leaving you only the ability to review unsubstantiated questionnaire answers. Are they among the organizations that expose IoT devices to the Internet? Do they adequately configure and protect those devices? RiskRecon objectively verifies vendor cybersecurity risk performance, enabling your analysts to see how well your vendors actually implement and operate their risk management program.

Mergers and Acquisitions

Know exactly what you're acquiring. RiskRecon delivers objectively gathered information about any company's information security program. You'll gain full knowledge of the environment and risks of an acquisition beforehand, enabling you to establish merger costs and potential liabilities with the Board and enter into the M&A process with greater peace of mind.