The Internet of Things isn't coming.

It's here.

PRODUCED BY:

Webtorials

STEVEN TAYLOR
Editor-in-Chief

Sponsored by ForeScout

The Internet of Things (IoT) isn't coming. **It's here.**

The Internet of Things (IoT) often seems to be a futuristic and exotic concept. The "Things" conjure up images of robots, self-driving cars and automated workplaces. Take a quick trip around the Internet and you find discussion of "smart pills" that transmit information when they contact stomach acid to record the time and the medication. You'll hear about biochip transponders on farm animals. Smart cars will be loaded with sensors ranging from mechanical updates to actually being self-driving. We even see "smart trashcans" that will send a signal when they need to be emptied.

But our world is already loaded with Things. And, as in life, it's often the Simple Things that matter most. Consider the lowly printer as a case in point.

For decades, a printer was no more than an automated typewriter attached to a computer. There was no inherent intelligence, and very little complication. But then came an evolution to multifunction and networked devices. Scanning, faxing and copying capabilities were added, along with both wired and then wireless networking. As with all other devices, the increase in options and capabilities comes with a commensurate increase in complexity and processing power. And this complexity and processing power means that rather than being an extension of a well-controlled computing device, the device itself is an integral part of the network, and, as such, it must be secured.

So what makes a printer—or any other Thing—a thing rather than a computer? One of the primary distinctions is the lack of a well-defined user interface and an accompanying ability to have full-blown security and/or security agents present.

In the words of the Bard, "Ay, there's the rub." We are rapidly evolving to a network where we have vast numbers of "computing devices" that are inherently unsecured.

So what to do?

That's what we asked members of the Webtorials Community and students from The SIP School in March and April of 2016. The respondents to the survey tend to represent the technological elite in IT and Telecommunications, and this analysis consists of only those who self-identified as a "professional involved in some aspect of installing, operating, planning and/or designing an enterprise communications network." The sample represented a wide range of company sizes from around the world across a broad range of markets.

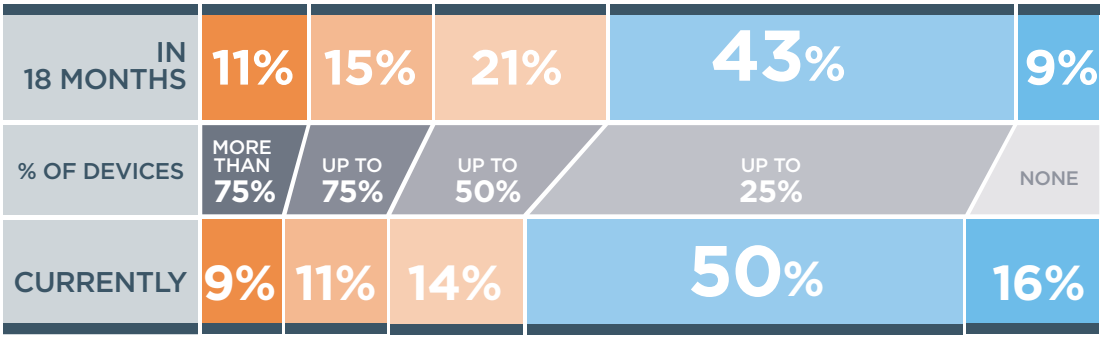
As you will see in the following pages, IoT is indeed here, and it is unsecured to an alarming extent.

Where are the Things?

THING 01

Even though respondents see growth coming in IoT devices on their networks, the current perceived penetration is quite low.

What percentage of devices on your network do you believe are non-traditional / IoT type devices?



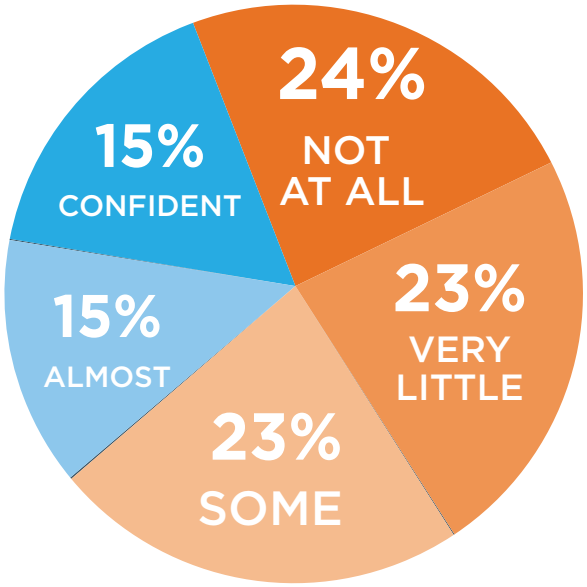
Two-thirds of the survey respondents feel that fewer than 25 percent of the devices on their network are Things. However, over the next 18 months, that percentage drops by half. The largest growth (50 percent) is in the 26 percent to 50 percent segment

The bottom line is that even though the current perceived percentage of Things is relatively low, Things are definitely on the radar, and respondents see strong impact in the offering.

THING
02

But very few are confident that they really know what Things are on the network.

How confident are you that you know all the IoT devices that are connected to your network as soon as they are connected and that you can control these IoT devices so cybercriminals can't use them as doorways into your network?



***85%** are not confident that they know all the devices on their network.*

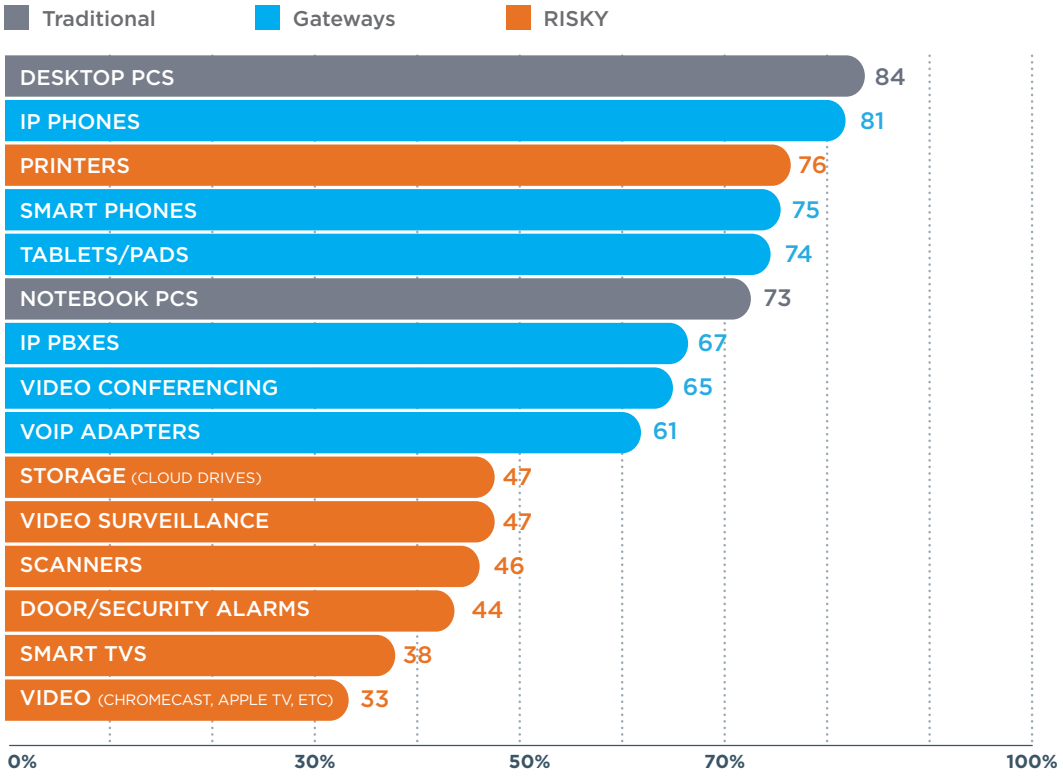
We hypothesize that a major reason there are so few Things on the network is because the respondents simply don't realize that they are there. Fewer than a third had a reasonable degree of certainty that they knew about and could control all of the Things as soon as they connected to the network. And almost half had little to no confidence.

THING
03

So we decided to put them to the test...

We asked which devices people had on their networks. And we included 27 sample IoT devices.

Which of the following device types are connected to your network (that you are aware of)?



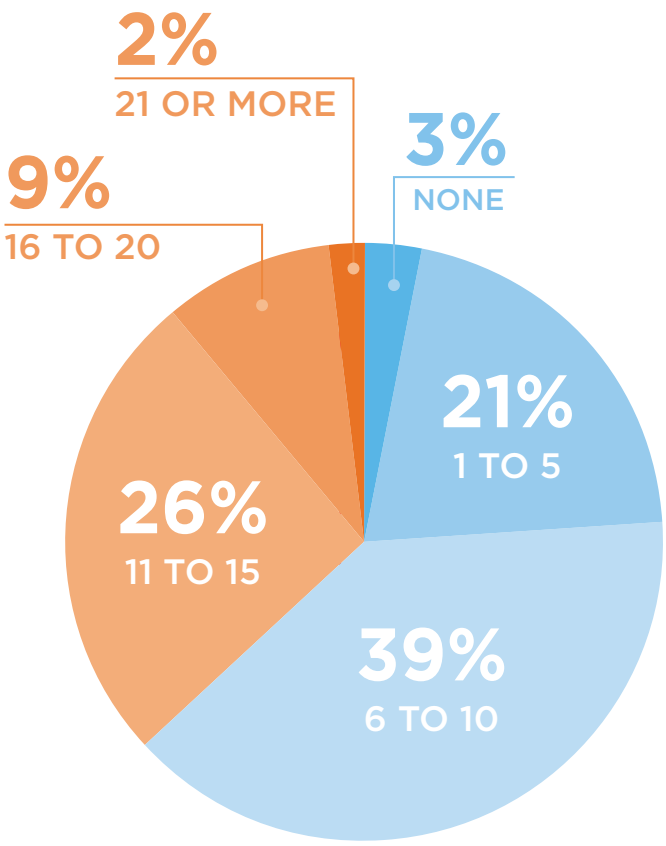
The survey included a list of a sampling of 29 devices that might be on the network – twenty-seven of which we consider to be Things. The devices shown here were the most prevalent choices. (The list of devices was randomized for each participant.)

Our classification here is that the grey bars represent devices that are traditionally included in a security strategy. Blue bars represent devices that should be considered in an IoT security strategy. Even though they may have a decent user interface, they also can contain extensions and apps that are not secured and can be a gateway into the core network. The devices represented by orange bars are the most worrisome in that they are, for the most part, not covered by any traditional security methods.

THING
04

The respondents couldn't change their initial answers. And they had an average of over nine IoT device types on their networks!

Number of IoT Devices per respondent - All respondents



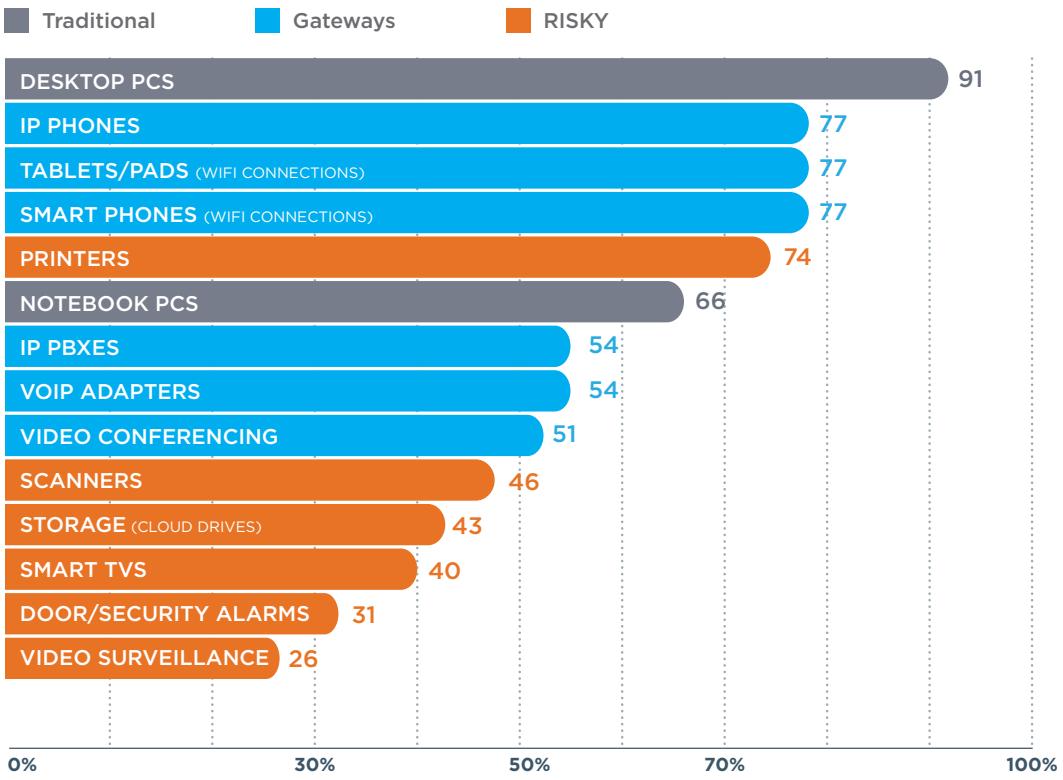
When the results were tallied, less than a quarter of the respondents had five or fewer device types. And almost two-thirds had six to 15 unique device types on their networks.

The survey was structured such that, after an initial answer concerning the proliferation of Things in the network, the respondents were not able to go back and change their answer after seeing our list of devices to jog their thinking.

THING
05

Then we looked at the respondents who said they had no IoT devices on their network. And they had almost the same profile.

Device Types for Users with “No IoT Devices”



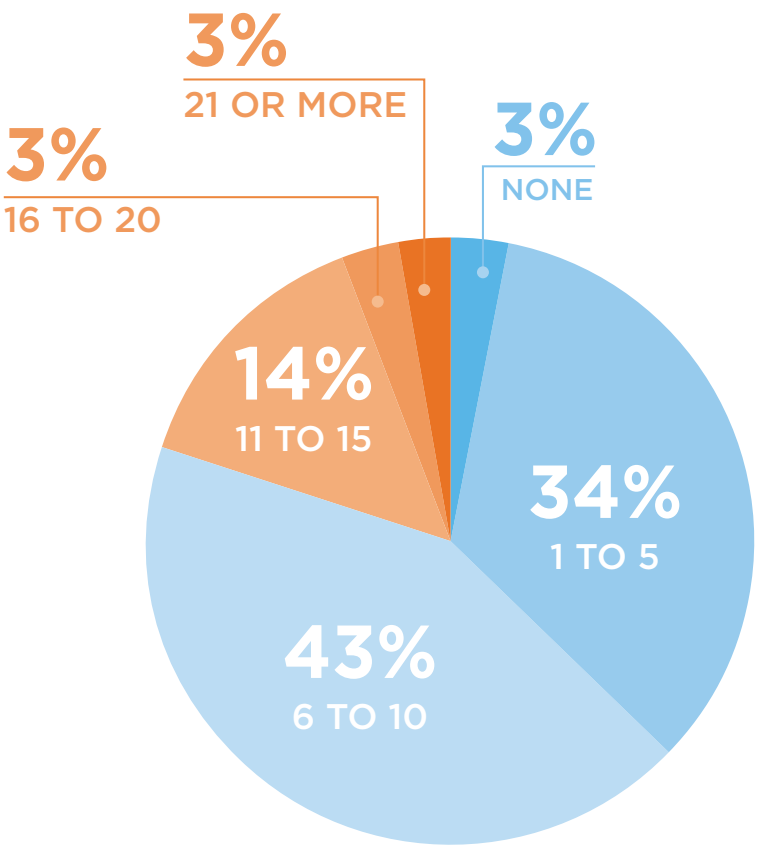
There was no significant difference between those who said they had at least some IoT devices on their networks and those who thought they had “none.”

Three-quarters of these respondents had three device types that we would consider as gateway threats and also highly risky printers. And roughly half had additional device types that are risky or gateways.

THING
06

And they had almost eight IoT device types on their networks.

Number of IoT Devices For those with "No IoT Devices"



Among respondents who initially said they had no Things, they averaged almost 8 IoT devices when queried.

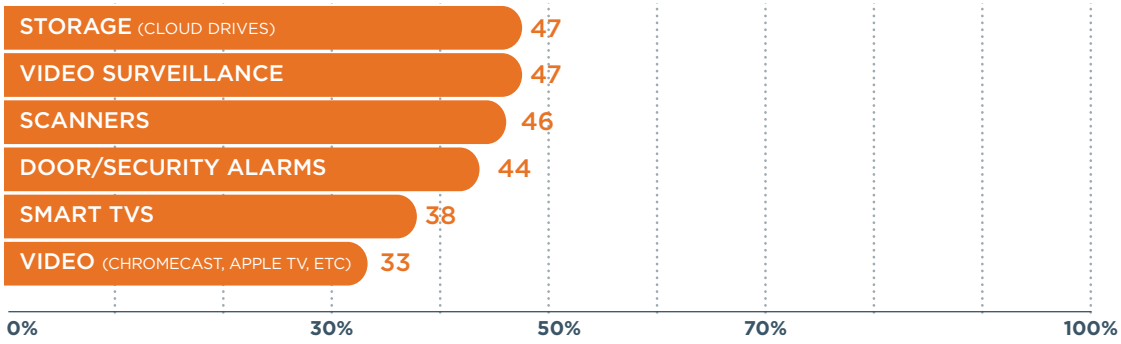
There was no significant difference between those who said they had at least some IoT devices on their networks and those who thought they had "none." In fact, the average number of IoT devices among the respondents with "No IoT Devices" was almost eight, as compared with a little over nine overall.

And contrary to what one might expect, the "No IoT Devices" respondents were not all from small companies. In fact, when this subset is compared with the sample as a whole, the distribution of how many devices they had was essentially the same.

THING
07

Additionally, there were significant, but smaller, numbers of other IoT devices.

Additional IoT Devices Found



Fewer than 25 percent of the respondents also had a wide range of additional IoT devices, all of which we consider high security risk.

While one might be tempted to see this as a low number—and low risk—it only takes one device from one category to compromise your network. It is important to note that some of these devices are just becoming popular and should be much more common in the future.

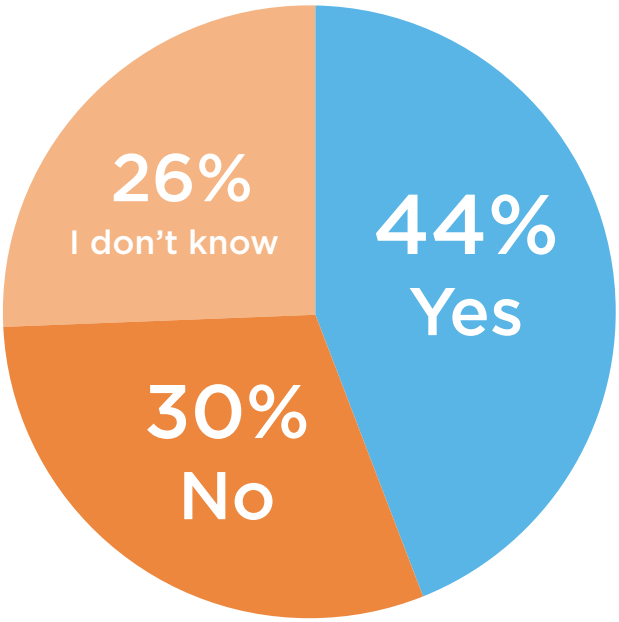
Additionally, some, such as point-of sale, SCADA and medical devices, are specific to a given industry. Thus, even though there may be a small percentage shown here, this likely reflects a small percentage of the overall responses being from these industries, and the usage could be nearly ubiquitous within the industry itself.

Securing Your Network of Things

THING
08

But how are IoT devices treated from a security perspective? They aren't.

Does your company have a security policy on IoT devices?



Only 44% of the respondents had a known security policy for IoT.

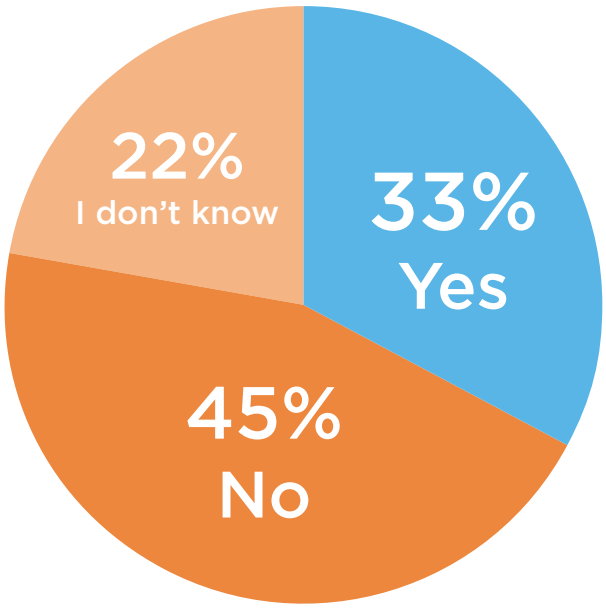
Fewer than half of the respondents have a security policy that includes Things.

And while this is surprising, it is even more surprising that a quarter of the respondents didn't know whether their security policy included IoT devices. In fact, some of those in the "I don't know" and "No" categories might not even have a security policy—since the policy would not include Things if none existed.

THING
09

And even fewer have a security policy that extends to home networks — a major potential entry point.

Does your company's security policy (if any) cover home networks (and by extension, devices such as home automation, thermostats, etc.) when accessing the corporate network from home?



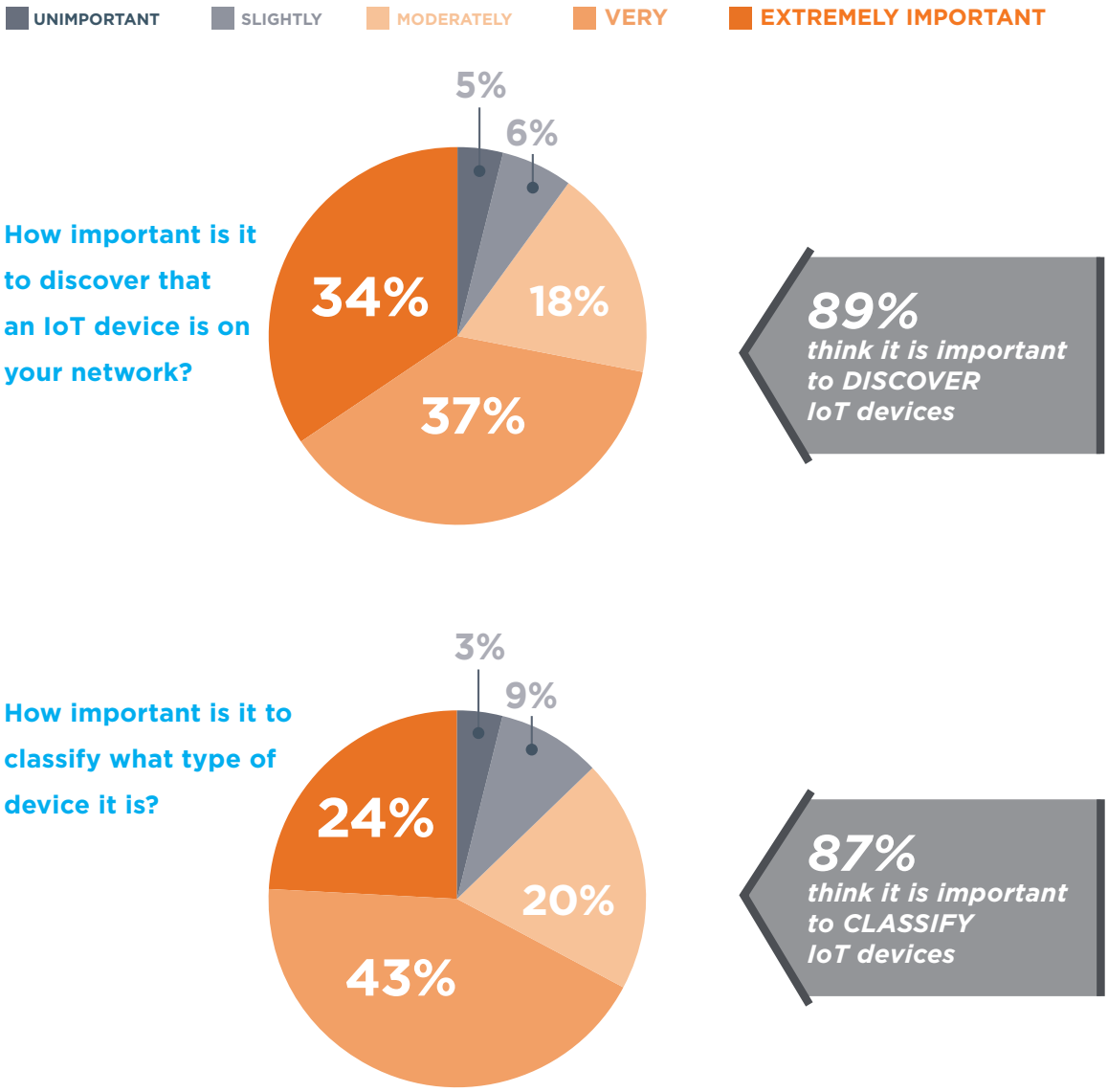
Only 33% of respondents are aware of their company's at-home security policy.

As the statements that we should be shocked by—but probably aren't—continue, only a third of the respondents have policies that include home networks. This is especially troublesome because—commensurate with the general lack of control for Small Office/Homes Office nets—one of the first widespread implementations of the IoT is in the "intelligent home."

This coupling of the increasing trend for mobile workers using their own network, the general lack of assumed IT sophistication among these workers and the proliferation of inexpensive "bare bones" devices makes for a most worrisome situation.

THING
10

We then asked about the importance of discovering, classifying and using agentless discovery. The importance far outweighed the extent to which anything is being done.

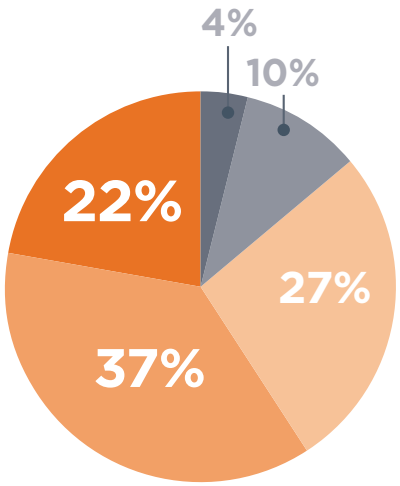


It comes as no surprise that the respondents, when asked to think about it, find discovering, classifying, and discovering/classifying without the use of an agent to be quite important. In fact, a very high percentage found this to be either "Quite Important" or "Extremely Important"—with 71 percent giving these ranks to discovery.

THING
10

UNIMPORTANT SLIGHTLY MODERATELY VERY EXTREMELY IMPORTANT

How important is it to discover and/or classify WITHOUT use of an agent?



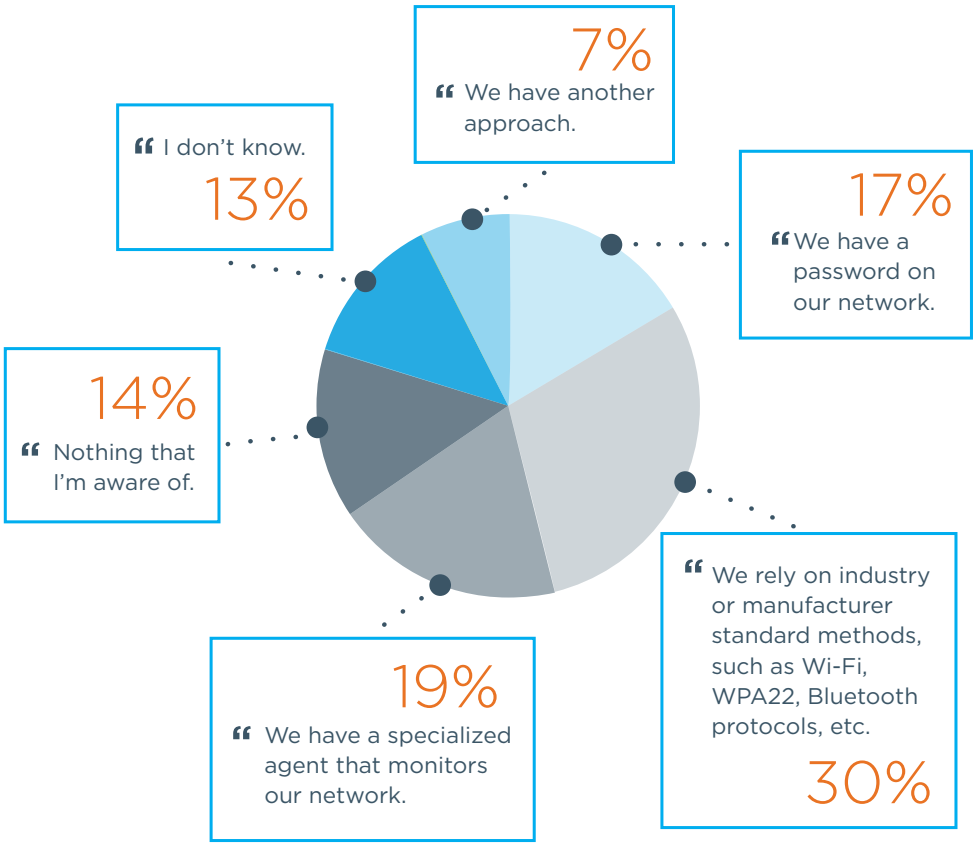
86%
think it is important to DISCOVER/CLASSIFY WITHOUT using an agent

As the world of IoT evolves quickly, agentless discovery and control is essential. The vast majority of Things are developed as extremely targeted devices with an extremely minimal user interface (to the extent that sometimes it is virtually non-existent). Adding the complexity and capability of embedding a security agent can hardly be expected in many cases, much less assumed.

THING
11

And mostly ineffective methods are being used for securing IoT...

Which of the following most accurately described your organization's current primary approach to securing IoT devices on your network?



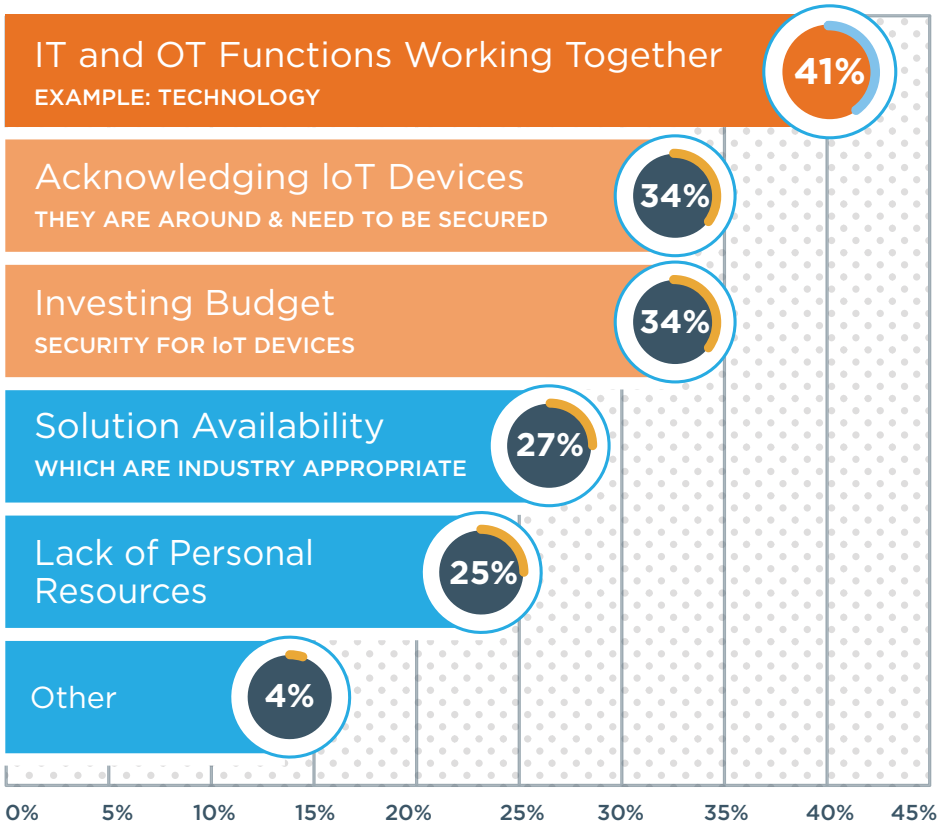
The bottom line here is that when Things are being secured at all, they are being secured with traditional methods that were designed for intelligent computing devices. Securing the IoT requires a new paradigm, and it is not yet in use.

Passwords and similar security is used in almost half of the instances. Only 19 percent use specialized agents—which still—as noted above—are largely nonexistent for Things. And fully 25 percent either don't know or know that they use nothing. Those in the "other" category generally indicated some form of variation on the choices offered.

THING
12

For reasons other than simply technology.

Which of the following do you believe will be your organization's *one or two biggest* challenges around IoT Security?



Providing appropriate IoT security is a massive challenge. However, technology is only a small part of the problem.

In this case, the respondents were only allowed to choose one or two issues as major problems, so the number of respondents who see each individual issue as a leading inhibitor is likely understated here.

And while our industry historically cites a lack of budget and resources as a major inhibiting factor, IoT adds new challenges. The most important two factors here are a lack of coordination between various groups within the IT organization and—perhaps more shockingly—a simple realization that a problem exists.

So the message is clear:

The current perceived penetration of IoT devices is quite low, but the **respondents are not confident that their perception is accurate.**

When respondents were asked which devices were networked, **the current penetration of IoT devices is actually quite high—and uncontrolled.**

But IoT devices, for the most part, are **not addressed as a part of the security policy—if a policy even exists.**

There is a dire need for advanced security—and for addressing hurdles to advanced security—including securing agentless devices.

Our call to action, then, is to educate ourselves and our colleagues to the **need for addressing IoT security immediately and to seek out products and services that enable this security.**

Or... as stated so elegantly...

Oh the Things you can find,
if you don't stay behind!

- Dr. Seuss

2016 Unified Communications, SIP, and SBC Plans and Priorities

This independent research report was commissioned by ForeScout Technologies.

About ForeScout Technologies

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of January 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.

Acknowledgment

Webtorials gratefully acknowledges the cooperation of The SIP School in the data acquisition phase of this report. The SIP School™ is owned by Vocale Ltd which was founded in April 2000 (Vocale Ltd is also the owner of the WebRTC School). It's SSCA® SIP training and Certification program has become recognized as the globally accepted Certification for VoIP professionals to strive for. Organizations such as the Telecommunications Industry Association officially endorse the program . Details of more industry supporting companies can be found at http://www.thesipschool.com/industry.html .

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products.

The primary author of this study is Steven Taylor, Publisher and Editor-in-Chief, Webtorials.

Published by Webtorials
Editorial/Analyst Division
www.Webtorials.com

Division Co-founders:
Jim Metzler
Steven Taylor

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.