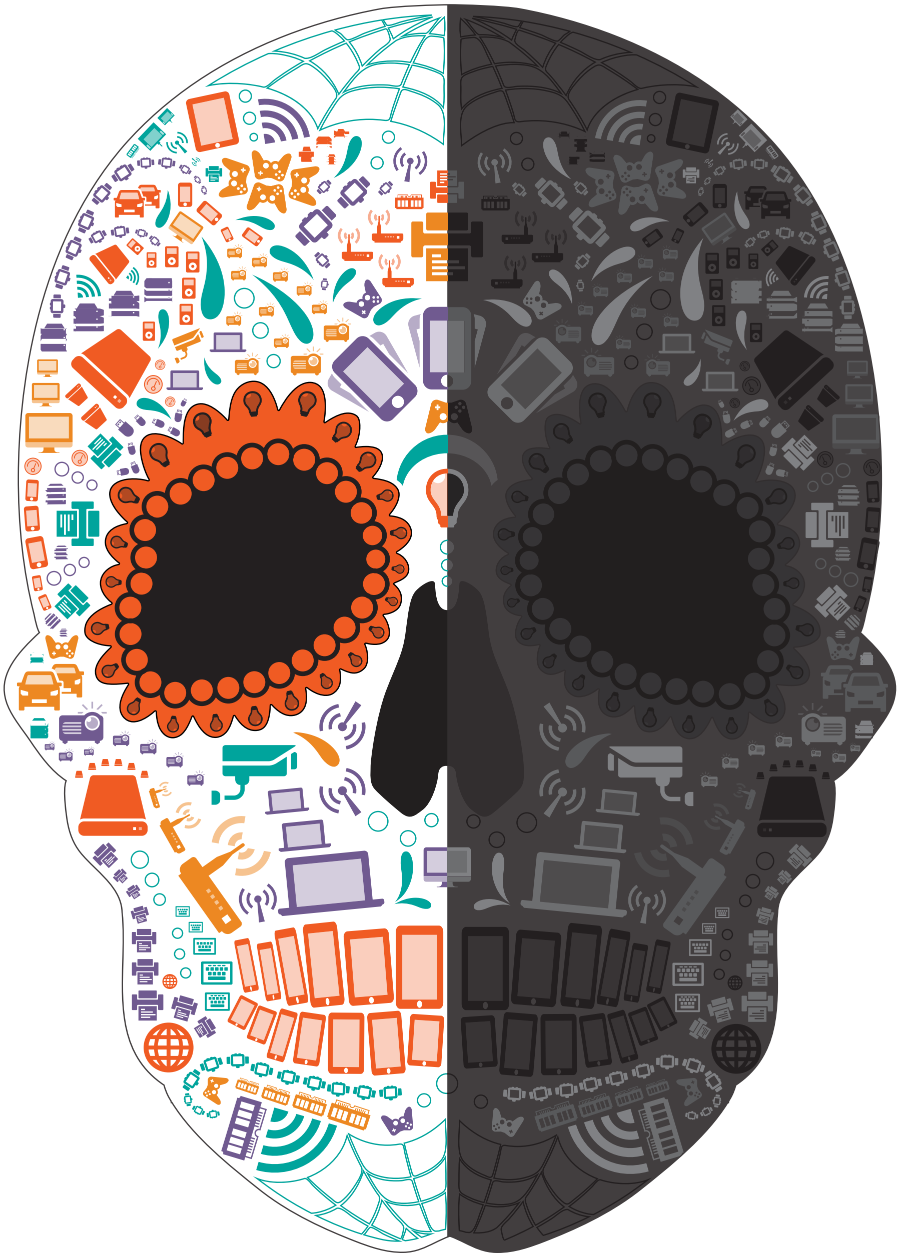
THE INTERNET OF EVIL THINGS®

2017

PERCEPTION | REALITY



PWNIE EXPRESS

@PwnieExpress

ABOUT THE REPORT

TRADITIONALLY, INFOSEC TEAMS HAD A DIFFICULT, BUT STRAIGHTFORWARD, JOB: THEY NEEDED TO UNDERSTAND THEIR ASSETS, KNOW WHAT THEY WERE CONNECTING TO, AND SEPARATE THEM FROM THE OUTSIDE WORLD.

That standard has changed, thanks to the many devices introduced into the workplace by employees, visitors, partners and other outsiders. Any device that can connect to a network, whether it is or isn't built to be malicious, can cause disaster to both the data and networks IT security is responsible for protecting.

So what exactly is The Internet of Evil Things®? First, we need to define evil, by which we mean malicious or harmful... purposefully or not. For the purposes of this report, we are defining a "connected device" as any device that can connect to a network or other devices via a wired or wireless signal. This frequently means Internet-connected devices, but Bluetooth and less traditional protocols are equally applicable.

This is the third year Pwnie Express researchers have studied the wired, wireless, Bluetooth, IoT, and BYOD challenges facing IT security professionals in the workplace. The report's findings were culled from a survey of more than 800 IT security professionals and on-the-ground data from Pwnie Express sensors monitoring real life wired, wireless, IoT, and BYOD device data gathered from a wide range of businesses across industries including financial services, hospitality, retail, manufacturing, professional services, technology, healthcare, energy and more. In the pages ahead, we will look at new insight from IT security professionals on many of the connected device concerns that we tracked in the 2016 IoET®, including an extensive look at bring your own devices (BYOD). But first, we will detail the results from new questions which look at one of the biggest, most significant attacks of last year and how it has changed IoT security forever.

TABLE OF CONTENTS

TABLE OF GRAPHS

EXECUTIVE SUMMARY

THE PWNIE EXPRESS RESEARCH TEAM SURVEYED 868 IT PROFESSIONALS—DOUBLING 2016. We looked at more than 10 times the number of wireless devices, now up to 74.5 million, and approximately 86 million connections from different kinds of devices, total.

The survey findings show that the InfoSec community is well aware of the vulnerabilities and risk that connected devices present. However, awareness is not leading to the actions and investments that will mitigate risk, secure enterprises, and ensure that the promise of a safe, connected world is realized.

Key findings include:

- 84% said Mirai changed their perceptions of IoT device threats.
- 66% of respondents said they either haven't checked or don't know how to check their devices for Mirai.
- One in five of the survey respondents (20%) said their IoT devices were hit with ransomware attacks last year. 16% of respondents say they experienced man-in-the-middle attacks through IoT devices.
- 92% think connected device threats will be a major security issue in 2017.
- 66% don't know or aren't sure how many connected devices their colleagues bring into work.
- Only 23% of the IT security professionals that monitor connected devices coming into their offices said they also checked those devices for malicious infections in the last year.
- Companies have not stopped producing products with insecure default configurations. The default network from common routers "linksys" and "Netgear" were two of our top 10 most common "open default" wireless SSID's (named networks), and the hotspot network built-in for the configuration and setup of HP printers—"hpsetup"—is still near the top at #2.
- IT security teams said they don't have the necessary tools to detect the risk of employee devices brought to the workplace. 41% of companies have no bring your own device (BYOD) policy while nearly 1-in-3 of respondents who have a BYOD policy have no way of enforcing it.
- Bluetooth devices in the enterprise are no longer theoretical: we detected them at workplaces, health centers, and industrial centers around the United States. We observed many types of devices, from Bluetooth styluses, smart TVs, and headsets to location devices like Tile.

- The number of IT security teams that have a budget for IoT security was up 11% from last year (see: The Biggest Changes in 2016 section below). However, there are more organizations with no IT security budgets than those with budgets for either IoT or BYOD security.

Looking at these results, we noticed an increasing number of professionals are aware and concerned about IoT, connected device, and BYOD risks. While perception is changing, the ability to address these problems is not evolving as quickly. Budgets are not keeping up with the needs of security professionals on the cybersecurity frontlines and huge numbers of insecure devices are being introduced to the enterprise. While 2017 reflected many of the trends we saw in 2016, the clearest changes are in perception, not implementation.

THE BIGGEST CHANGES IN 2016

- **44%** responded that they care more about device threats than traditional network security—up **16%** from 2016.
- Respondents with a BYOD policy in place is actually down **8%**—(**63%** last year vs. **55%** now).
- The number of respondents that have a budget or plan to have a budget for IoT security is up **11%**, but budgets for IoT remain low compared with other categories and are much lower than the fear IT security professionals shared about IoT security.

INTRODUCTION

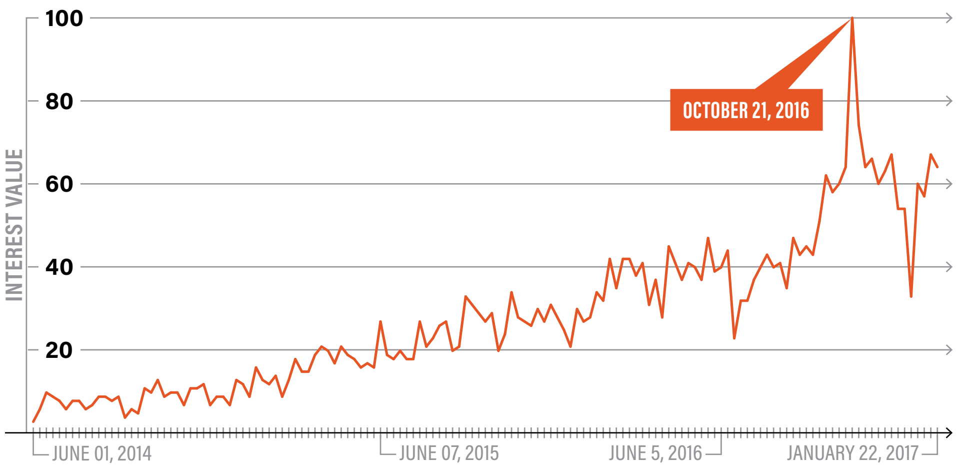
IN 2015, THE RISK FROM CONNECTED DEVICE THREATS WAS A HOT TOPIC FOR DISCUSSION. In 2016, the discussion became a reality, with top InfoSec minds demonstrating at conferences like DEF CON how rogue actors could take advantage of products of all kinds—phones, locks, cars, and more. Then came October 21, 2016. The Mirai-fueled zombie botnet army was deployed on Dyn, one of the world's largest DNS providers, taking down internet access in many of America's largest cities. Mirai gave the entire world just a glimpse of how vulnerabilities in Internet of Things (IoT) devices can be exploited to disrupt business, consumers, and organizations around the world and slow the internet to a crawl.

Today's threat landscape required our third edition of our Internet of Evil Things (IoET®) to be different than the two previous IoET® reports. For the 2017 IoET® report, Pwnie researchers set out to inquire how Information Security (InfoSec) professionals and the organizations they work for are adapting to a new reality.

The first result that caught our eye: concern about device threats is now considerably higher than concern over traditional network security (44% to 21%—a 23-point difference). InfoSec professionals used to managing the risks from wired and wireless devices—like the phones in our pockets, computers controlling critical infrastructure, as well as printers and access points employees bring in to increase their productivity—face new challenges. We now work in offices where the conference room whiteboards are smart, security cameras are wireless, and speakerphones are Bluetooth. Even the coffeemakers are connected and can potentially open a backdoor to a rogue actor.

Our 2016 report focused on the introduction and growth of the IoT and connected device risk. The October Mirai attack raised global awareness to a level more in line with industry-expert awareness. Consider for a moment the number of people who searched for "IoT security" last year. The graph below shows Google's interest over time number for IoT Security.[i] Clearly October 21 was when the world went to Google to find out about Mirai.

GRAPH 01 **IOT SECURITY SEARCH INTEREST TREND**



[i] Definition of "interest over time" from Google: Numbers represent search interest relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. Likewise a score of 0 means the term was less than 1% as popular as the peak.

Other related Google search terms saw similar spikes, including "protecting IoT," "botnet," and cybersecurity."

The attack of the botnet army changed the Info-Sec world forever. A massive zombie army, controlled by rogue actors exploiting vulnerable IoT devices, is no longer just a theory. In this year's report, Pwnie Express researchers reshaped the survey to take into account the Mirai attack and look at how prepared security professionals are for connected devices—including IoT and BYOD—in the workplace.

We saw differences right away:

The first noticeable finding is fear. InfoSec professionals are clearly worried about the expanded attack surface and the risk the increasing number of connected devices in the workplace have introduced:

- Nearly 90% said they are concerned about IoT vulnerabilities;
- 44% said they are more concerned about device threats than traditional network security—a 16% increase from last year;
- More than 90% said connected device threats will be a major issue in 2017. That's up almost 7% from last year;
- Almost two-thirds of the security professionals said detection and mitigation of rogue, unauthorized, and malicious devices was a priority for their security programs.

But elevated concern has not yet translated into action.

More than 66% of respondents said they don't know how many connected devices come into their offices. Worse, of those who know how many connected devices enter the workplace, about one-third have never checked or are not sure when they last checked for malicious infections. It's likely that these pros have similarly not checked for a breach or other compromise.

The good news: More people are aware of the danger from attacks via IoT connected devices and devices employees are bringing into work.

The bad news: Budgets and action "on the ground" are not growing as quickly as the concerns of the professionals. Professionals acknowledged there are huge holes in their companies' defenses, while InfoSec teams do not yet have the resources to address the problems.

TOP 3 DEVICE THREATS OF 2017

In comments from survey respondents, the most commonly mentioned threats of concern included:

- → Misconfigured healthcare, security, and IoT devices that will provide another route for ransomware and malware to cause harm and affect organizations.
- → Unresolved vulnerabilities or the misconfiguration of popular connected devices, spurred by the security holes being publicized by botnets, including Mirai and newer, "improved" versions.
- → Mobile phones becoming an extra attack surface and another mode of rogue access points taking advantage of unencrypted Netgear, AT&T, and hpsetup[ii] wireless networks to launch man-in-the-middle attacks.

[ii] "hpsetup" is the default configuration of most hp printers.

IOT—LIFE AFTER MIRAI

ON OCTOBER 21, 2016, A MASSIVE DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK TOOK DOWN LARGE PORTIONS OF THE INTERNET ACROSS THE UNITED STATES. It quickly became clear that the only way an attack that large could have happened was with an unprecedented number of computers. In this case, connected devices like webcams were being used as unwitting accomplices in the biggest DDoS attack in history.[1] How were they being "recruited"? A clever malware that took advantage of unprotected, web-connected devices with weak or non-existent passwords. Like other botnets, anybody's devices could be a part of the zombie mob.

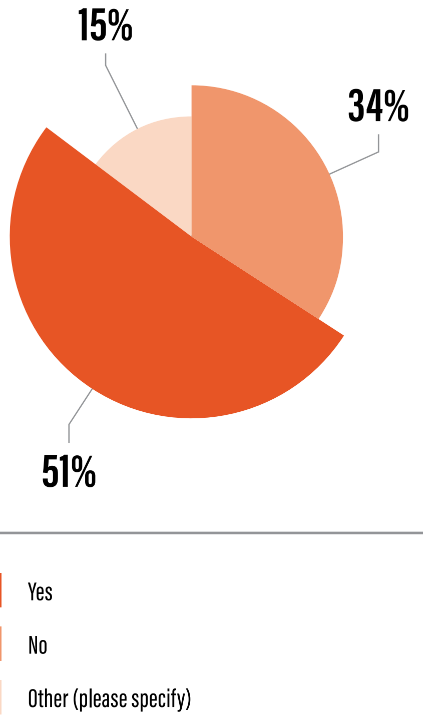
Unlike many previous attacks, the InfoSec world had to take notice. Within hours of the attack BuzzFeed, *The New York Times*, *The Wall Street Journal*, and many others published explanations of what might have happened. Our respondents made it clear that Mirai got their attention: 84% said the botnet changed perceptions of IoT device threats.

While Mirai isn't making headlines anymore, the fallout from the attack lingers. But for all the trouble that Mirai caused, few have addressed the fallout from the botnet attack. 66% of our respondents said they either haven't checked or don't know how to check their devices for Mirai.

"Historically, IT security has not worried about what they don't own or control. The Mirai attack points out that there are devices associated with your network or around your network that challenge IT security professionals in new ways," said Paul Paget, CEO of Pwnie Express. "Non-traditional IT, that may be controlled by a vendor or another organization, now has to be taken into consideration. This wasn't always part of security's mission, but Mirai has changed everything. These pros need reinforcements now more than ever as the number of security challenges surrounding enterprises continues to skyrocket."

When asked to describe their level of concern about vulnerable on-premise IoT devices, 60% of InfoSec pros said they were concerned. But many respondents indicated they don't have the tools to protect IoT devices in their office. Just 8% of our respondents said they could continuously monitor and detect off-network IoT devices in real time compared to 29% that could monitor threats from

GRAPH 02 **HAVE YOU TRIED TO DETERMINE IF THERE ARE DEVICES IN YOUR OFFICE THAT HAVE BEEN INFECTED WITH MIRAI?**



Number of respondents: 868

off-network WiFi devices. That means less than 1 in 10 IT security departments could detect Mirai on a webcam, a printer, or a device brought from home into an office. While IT security departments are more prepared to track on-network IoT (40% said they could monitor it), the number pales next to IT's ability to track real-time threats on traditional wired devices (76%) and on 2.4 GHz WiFi devices (70%).

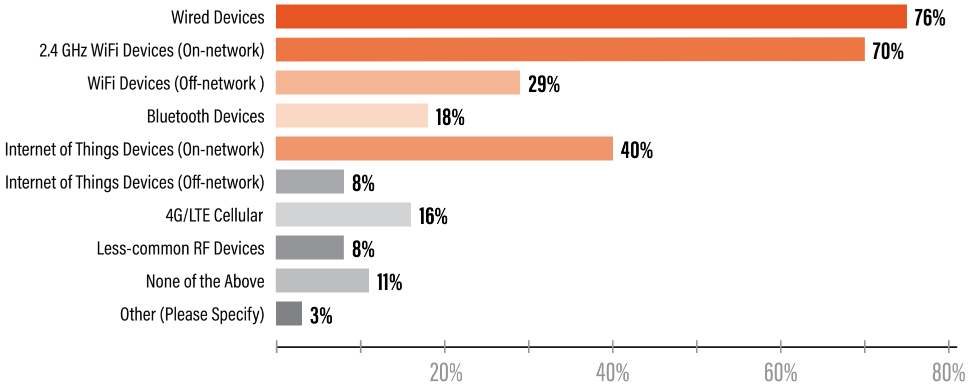
Also, the 40% of respondents that can continuously monitor and detect on-network IoT is down from 44% last year. Real-time detection levels are up in all other categories. The number of respondents that can continuously monitor and detect off-network IoT devices is essentially the same, despite detection levels being up in all other categories.

Yolonda Smith, director of product management at Pwnie Express, said this finding shows that "for most people, the threat hasn't become 'real' to them yet, despite published vulnerabilities which can lead to loss of life, loss of privacy, or loss of revenue. This perception makes it that much easier for organizations to turn a blind eye as these devices permeate every aspect of the business, increasing the likelihood of these threats having a devastating impact."

For those who say that Mirai didn't affect them or their devices, this thinking is shortsighted. First, attack traffic from Mirai affected many networks, even if they didn't have vulnerable devices. Second, if a rogue actor can use your network for a botnet attack today, it could be used for more sinister purposes tomorrow. Cyberattacks have hurt top brands and their carefully crafted images. One attack could alter the way consumers look at a brand for decades.

New attacks will force organizations to come up with new countermeasures to address evolving threats. While the Mirai attack knocked sites like Twitter, Netflix, and Spotify down for hours, it didn't affect the devices used to launch the attack. For most Americans, it was an aggravation, but not a crisis. The next attack is likely to be different. One in five of the survey respondents said their IoT devices were hit with ransomware attacks last year. Ransomware attacks—which strike the pocketbook and hurt a company's bottom line—should force organizations to get more aggressive in their efforts to protect their

GRAPH 03 **WHICH OF THE FOLLOWING ARE YOU CURRENTLY ABLE TO CONTINUOUSLY MONITOR AND DETECT IN REAL TIME?**



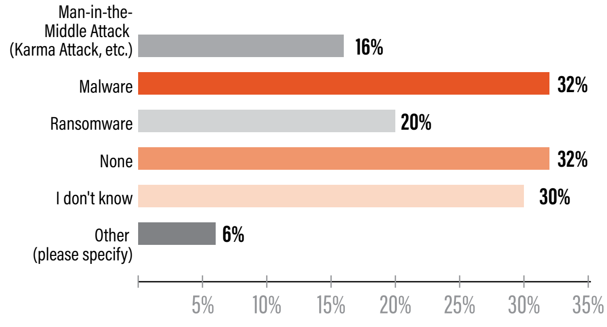
Number of respondents: 868

IoT devices. With technology distributed throughout businesses, these kinds of attacks will become more problematic. Recently, an Austrian hotel lost the ability to create new room keys due to a ransomware attack.[2] Just as amazing, 16% of respondents say they experienced man-in-the-middle attacks through IoT devices.

Pwnie Express InfoSec Ranger Jayson Street says it is a sign of how ransomware is growing and its developers are adapting. "Be it a smart television, a mobile device, or hospital equipment, ransomware has increased its attack surface in the last few months. It's no longer just PC's and surfing to a website that can compromise you. You now have to worry about other connected devices, where they're going to, and what they're communicating with." Ransomware passed on via IoT devices is another issue we plan to do more research on for a future report.

One sign that defending against Mirai is not just a matter of resources and staffing, but more about will—small businesses (those between 1-50 employees) were 8% more likely to have checked for Mirai than those at larger companies (with 1,000 or more employees). We'll take a closer look at how companies police their networks differently in an IoET® supplemental report later this year.

GRAPH 04 **WHAT TYPES OF ATTACKS HAVE HIT YOUR IOT DEVICES IN THE LAST YEAR? CHECK ALL THAT APPLY.**



Number of respondents: 868

MIRAI: PERCEPTION | REALITY

While 84% of respondents think that Mirai changed the perception of IoT device threats, only 34% have actually checked to determine if their devices are infected.

Respondents told us about some of the threats they are most worried about in 2017, both for their business and their personal concerns (IoT and Ransomware were the two most-used words this year):

→ **Business Concerns:**

- Brute force attacks on my WiFi networks
- IoT vulnerabilities
- Smartphone attacks
- WiFi and wireless vulnerabilities

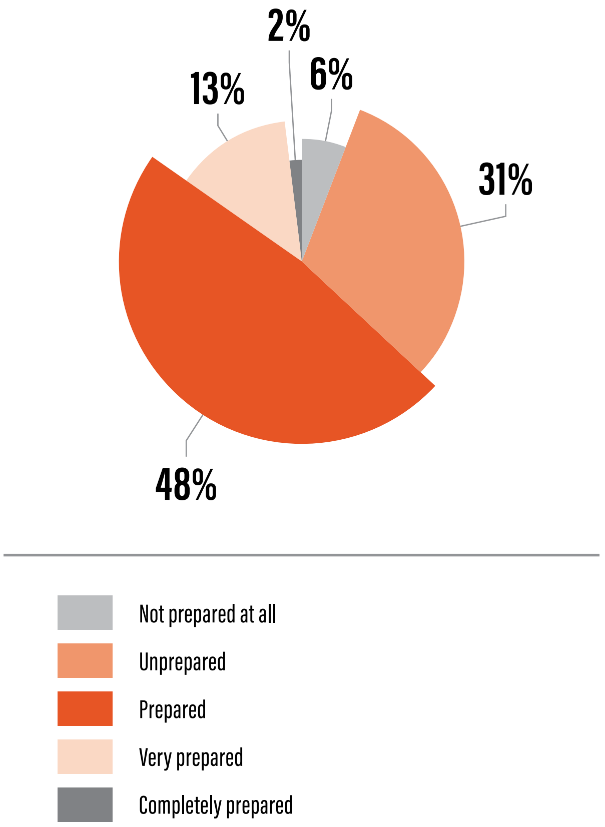
→ **Personal Concerns:**

- Wireless Cars
- Wireless home monitoring and safety devices
- Vulnerable connected children's toys
- Smart TV's

(IN)SECURE DEVICES

THE BOTNET THAT FUELED THE MIRAI ATTACK WOULD NOT HAVE BEEN POSSIBLE WITHOUT VULNERABLE DEVICES, BUT NOT ALL IT SECURITY PROFESSIONALS THINK THEY ARE READY TO SECURE THEIR ORGANIZATIONS AGAINST THESE ATTACKS. Almost half (48%) of respondents said their organizations were prepared to detect connected device threats, but more than a third (37%) of all respondents were unprepared or not prepared at all.

GRAPH 05 **HOW PREPARED IS YOUR ORGANIZATION TO DETECT CONNECTED DEVICE THREATS?**

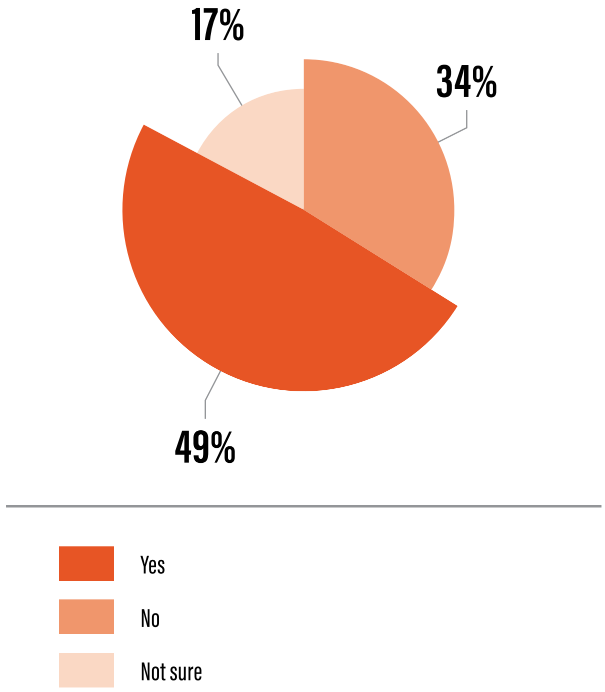


Number of respondents: 868

Still today, a fact that half of those surveyed thought they were prepared could seem like a good thing, considering the newer nature of the threat. But it seems that "prepared" might be a looser term than we had realized. When we got a bit more specific in our questioning, the numbers took a turn for the worse. Asked specifically whether they knew how many connected devices came into their offices, two-thirds didn't know.

When we pressed the one-third who said they could see what connected devices were coming into their offices, nearly 1 in 3 said they have not checked

GRAPH 06 **DO YOU KNOW HOW MANY CONNECTED DEVICES YOUR EMPLOYEES ARE BRINGING INTO WORK?**



Number of respondents: 868

employee-connected devices for malicious infections, despite awareness of unidentified connected devices entering their workplace. InfoSec teams should be checking employee connected devices for malicious infections at least once a month, but only 28% of all respondents had checked in the last month for malicious infections.

Only 23% know what connected devices their employees are bringing into the workplace AND have checked those devices for malicious infections in the last six months.

Chris Wysopal, founder and chief technology officer of application security company Veracode, told us: "Consumers and organizations don't know how to manage the risks associated with connected devices. They don't know what's vulnerable, how to find out, or what to do about it. This target rich environment will be irresistible to criminals seeking to monetize our vulnerable devices."

We obviously would like to see security pros gain a better sense of what is coming into the office and run more frequent checks for incoming malicious materials. Survey results clearly point to an increasing awareness of rising security risks:

- 74% are extremely concerned or concerned about devices in a default, misconfigured, or vulnerable state.
- 51% are extremely concerned or concerned about the threat that malicious hardware (wireless keyloggers, RFID cloners, skimmers, etc.) pose to their networks.
- 48% are extremely concerned or concerned about the threat to their network from wireless physical security systems (cameras, locks, alarms, etc.).
- 46% are extremely concerned or concerned about 4G/LTE hotspots and cellular broadband USB dongles near their networks.

> "CONSUMERS AND ORGANIZATIONS DON'T KNOW HOW TO MANAGE THE RISKS ASSOCIATED WITH CONNECTED DEVICES. THEY DON'T KNOW WHAT'S VULNERABLE, HOW TO FIND OUT, OR WHAT TO DO ABOUT IT. THIS TARGET RICH ENVIRONMENT WILL BE IRRESISTIBLE TO CRIMINALS SEEKING TO MONETIZE OUR VULNERABLE DEVICES."
>
> —Chris Wysopal, Founder and Chief Technology Officer, Veracode

The zombie botnet army attack has opened eyes not just to IoT vulnerabilities, but to all connected devices and the harm they can cause to existing networks. The existence and spread of the Mirai malware suggests that despite industry concerns about vulnerable hardware, InfoSec professionals are not confident about the security of connected devices and configuration standards.

In the recently published Gartner report, "Real-Time Discovery, Visibility and Control Are Critical for IoT Security," authors Saniye Burcu Alaybeyi and Lawrence Orans wrote: "Based on recent Gartner inquiries and vendor briefings, the lack of IoT network and device visibility is now a top concern of chief information security officers (CISOs), both in consumer and industrial IoT verticals. Discovery is considered a prerequisite to IoT security."3

TRENDS IN INSECURE DEVICES:

Pwnie Express has the proprietary data and technology to observe and analyze trends of insecure devices in enterprises around the world. Using a series of network sensors across more than 650 locations from a wide range of businesses across industries including financial services, hospitality, retail, manufacturing, professional services, technology, healthcare, energy and our own Software as a Service (SaaS) device threat detection platform, the Pwnie team has unique insight into not only the devices these sensors see, but their configuration settings, vulnerabilities, and behavior. These sensors are all placed in business and industrial (non-residential) settings, but can see devices in surrounding areas as well: the major areas of concern for those who need to understand the entire attack surface. More importantly, this data gives us a better sense of new device concerns on the horizon including man-in-the-middle attacks, Bluetooth devices, and other potential wireless attack vectors.[iii]

1. VULNERABLE WIRELESS ACCESS POINTS

According to traditional network security mindset, a properly segmented network and careful configuration should protect organizations from things like man-in-the-middle attacks. This is clearly not the case: 18% of the 2017 survey respondents mentioned that their employees' wireless devices had been affected by man-in-the-middle attacks.

> "AS A TARGET RICH ENVIRONMENT FOR IOT AND TRADITIONAL COMPUTING DEVICES, THE ABILITY TO MONITOR, AUDIT, DETECT, AND NOTIFY OF THE PRESENCE OF SUSPICIONS WIRELESS DEVICES IS THE CORNERSTONE OF ANY IOT DEFENSE-IN-DEPTH SOLUTION."
>
> —Larry Pesce, Director of Research, InGuardians

The lack of proper configuration and encryption were particularly surprising as a full 21% of all viewed SSIDs had weak or no encryption—far beyond what would be expected in an enterprise environment. 18% of these service set identifier (SSIDs) had no encryption and a surprising 3% of all SSIDs had Wired Equivalent Privacy (WEP) encryption—a standard so outdated it was considered vulnerable a decade ago.[iv] Unencrypted and vulnerable networks do not properly protect the flow of information within the organization. While properly segmented

[iii] All analysis of the Pwnie data was done in a manner consistent with the agreements we have with customers and data was used in aggregate only. Personally Identifiable Information was removed before processing.

[iv] From https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy: Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network.[1] WEP, recognizable by its key of 10 or 26 hexadecimal digits (40 or 104 bits), was at one time widely in use and was often the first security choice presented to users by router configuration tools.[2][3] In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA).

networks can theoretically help protect employees using connected networks, frustrated employees with slow connections or guests with sensitive information can be tempted to use, and transmit information over, these poorly secured networks.

In addition, unencrypted wireless networks with common, familiar names create an extra threat—they allow rogue actors to easily set up man-in-the-middle attacks. Pwnie Express noticed that most of the top unencrypted networks used standard naming conventions such as "Netgear," "ATT," and "hpsetup." These kinds of insecure network connections can happen even in relatively secure environments, as they are frequently just the unconfigured, automatic hotspot generated by a newly installed router, printer, etc. While easy setup and connectivity is important, it also means that anyone can connect to that device.

Larry Pesce, director of research at InGuardians, said: "With the increase in use of IoT technologies, we are poised to see increased adoption of wireless technologies in our environment. In a target rich environment for IoT and traditional computing devices, the ability to monitor, audit, detect, and notify of the presence of suspicions wireless devices is the cornerstone of any IoT defense-in-depth solution."

2. BLUETOOTH DEVICE THREATS

Even if an organization can get a handle on the BYOD and office-issued gear, a surprising amount of standard office equipment is now Bluetooth-connected. Speakers, conference room equipment, and smart TV's are frequently Bluetooth-enabled and can provide another entrance onto your network. These devices can also be tricked into connecting to a rogue Bluetooth device with a commonly used or expected name.

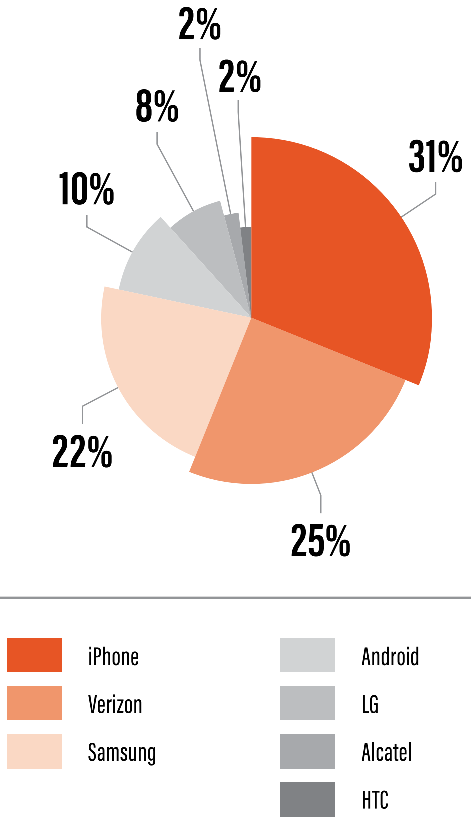
We detected more than 9 million Bluetooth devices in enterprise environments. Many of these devices are not vulnerable, but they were all present, suggesting the presence of personal hardware in the enterprise. Some of the most common Bluetooth device names that we detected were:

- Apple Pencil, Flex—both great examples of relatively innocuous Bluetooth "add-ons," the Apple Pencil and Flex (Fitbit) are also good examples of Bluetooth input and output devices—potentially detrimental to the device they are connected to, or in the case of headphones or speakers, possibly susceptible to eavesdropping.
- iPhone, LG Stylo 2 Plus—while iPhones and other smartphones like the LG Stylo are generally secure devices, any additional beachhead can prove to be dangerous. More importantly, a generic "iPhone" Bluetooth connection is likely to be approved by most devices, including those like conference room equipment that may have access to sensitive information.
- Bluetooth trackers—the Tile™ is a useful gadget that connects to things so that you can find them through an app on your phone—useful, and reasonably secure, but also common enough that an unsuspecting user might be tempted to connect to a not-so-innocent Bluetooth connection called "Tile." With more than 8 million Tiles sold and similar technology entering the market, the potential of a vulnerable copycat device entering the market is increasing. Tile provides the ability to "help others out" by finding their Tiles—very positive, until someone "helps out" your CEO

by finding his keys, for instance. Tiles are used for all the things people don't want to lose: keys, wallets, ID badges, phones, and more. These are a great example of the kind of persistent digital presence that is part of the growing challenge to enterprises.[v]

- General Motors—the Pwnie Express team detected more than 2,500 "General Motors" Bluetooth names alone, which shows that Bluetooth-connected cars are actively being used.

GRAPH 07 **MOBILE DEVICES USED FOR WIRELESS INTERNET ACCESS**



3. MOBILE DEVICES

Mobile phones are the attack vector of the future[4]: We are used to seeing mobile phones in the office. The security community has had to step up efforts to secure these small and powerful computers that have the potential to cause serious damage to established business networks, and provide yet another attack surface for data theft.

To the rogue actor, a phone is a beachhead that can be used to connect to a corporate network. The hacker doesn't care who owns the phone—the employee or the company—as long as it can be used to cause harm, through delivery of malicious payloads via email or compromising the network itself. A compromised phone has access to sensitive data within an organization. Mobile phones can now be used to provide internet connections, a terrific feature for workers annoyed with a slow or highly-restricted connection. While this functionality is useful, many often put productivity ahead of protection when they connect to unofficial networks. One of the most common "open by default" wireless networks that we saw, ATT, is an open network that many mobile users feel comfortable connecting to, making it a prime target for man-in-the-middle attacks.

Aaron Turner, an Independent IoT Security Researcher and Faculty at IANS (the information security advisory company), told us "as the price of connected components drops due to the commoditization of Bluetooth, WiFi, and LTE modem chips, criminals are integrating their own connectivity into their attack devices. For example, credit card skimmers once almost entirely required the criminal to physically retrieve the skimmer. Now, Bluetooth dominates the skimmer deployment model, with LTE modems rapidly gaining in numbers. The low cost of

[v] All attacks are theoretical, and examples of larger concerns with connected devices being present in the enterprise.

these components makes it attractive for criminals as it reduces their risk and also helps them scale their criminal operations."

Because mobile access points are an extra attack surface, we used the sensor data to assess what kinds of mobile devices were being most frequently used in and around enterprises.

However, we were pleasantly surprised to see fewer mobile hotspots on our list of "unencrypted" or "poorly encrypted" Wireless Access Points.

4. NON-TRADITIONAL CONNECTED DEVICES AND MALICIOUS HARDWARE

A whopping 84% of our respondents were somewhat to extremely concerned about the network threat from wireless physical security systems, devices that have not traditionally posed a problem to the integrity of the network security program. Also, malicious hardware has made a comeback: with non-traditional devices like wireless keyloggers getting their own "wanted" posters from the FBI, organizations have become aware that connected devices can be built to infiltrate or take down a corporate network.[5] The Raspberry Pis found across the locations we looked at suggest that malicious hardware is still present. While Raspberry Pis have useful purposes, their presence on or near corporate networks with wireless turned on is definitely not a good sign. Even if they are not being used as malicious hardware, their built-in security is not sufficient for enterprise use.

In addition, Pwnie Express found connected Nest devices, wirelessly-connected drones, and a number of wirelessly-connected healthcare and industrial control devices on or around the networks of these office environments.

"A big component of the risk from IoT stems from the requirement of constant, persistent connectivity, both between devices as well as out to the Internet," said Yolonda Smith. "Keeping connectivity at the forefront of the requirement means that security inevitably takes a backseat as we saw with Mirai."

CONNECTED DEVICE THREAT: PERCEPTION | REALITY

Even those who are aware of connected device risks often are not fully aware of the real dangers they pose to the network. Even fewer know how to address the problem.

- 92% think connected device threats will be a major security issue in the coming year.
- Only 57% know how many devices are connected to their networks.
- More than a third (37%) are not prepared to detect device threats and 35% are not prepared to respond.

→ **More professionals are witnessing in the wild attacks:** 57% of respondents said they have witnessed an attack via a wireless device, up 3% from last year and clearly something that IT security pros are seeing in their own environments.

CAN I-T SEE BYOD?

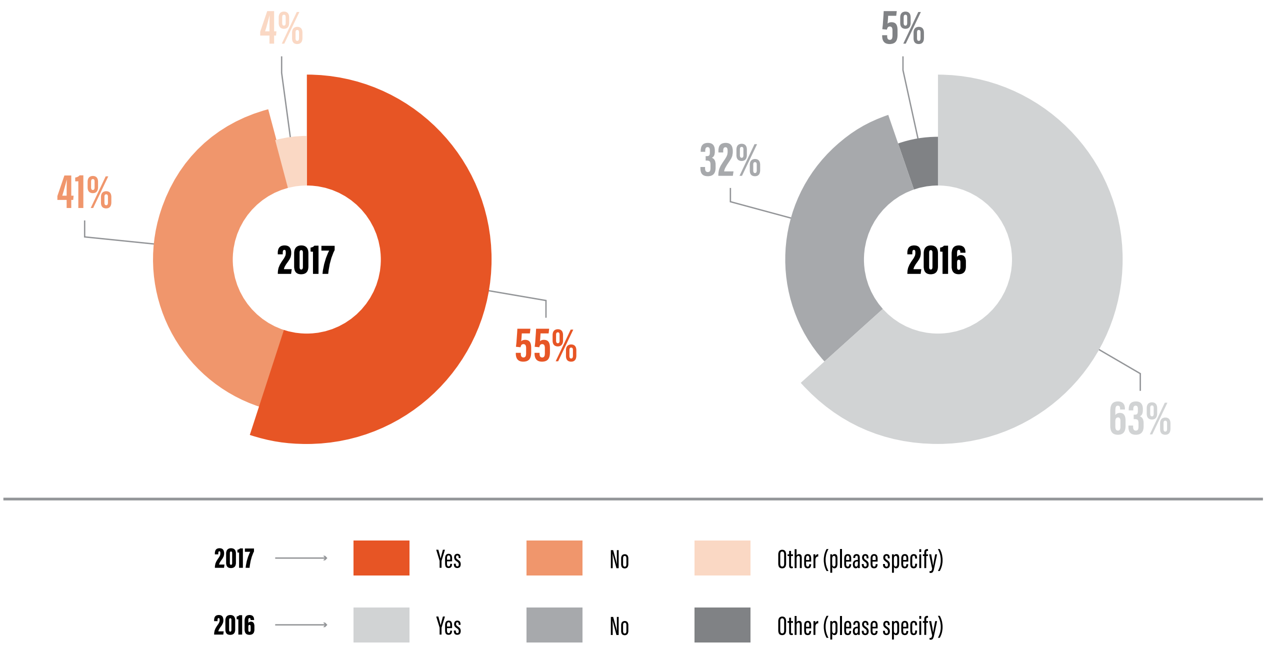
MANY IT SECURITY EXPERTS CAN'T SEE WHAT'S COMING INTO THE OFFICE. The problem is not just personal devices meant for personal use. Increasingly, individuals are purchasing work devices on the company dollar, meant to be used on company networks, for company purposes. These BYOD policies are being implemented to reduce costs and create happier employees, but the policies make security more difficult. We also found many offices don't have clear guidance on what devices can come into the office and how they should be configured. The devices that employees bring in and out of the office every day have the potential to cause serious harm to company data, and the 2017 survey showed just how concerned the pros are. 72% showed concern about corporate sponsored BYOD programs pose to their network.

And their offices may not have the proper procedures in place to secure devices:

- 55% of respondents said their organizations have a BYOD policy in place. That's down 8% from last year—one of the biggest changes we saw in the research from last year.
- Nearly 1 in 3 respondents who have a BYOD policy have no way of enforcing it;

"While the state of IoT security is poor, and has been for some time, the attack surface is increasing as employees continue the BYOD trend," said Paul

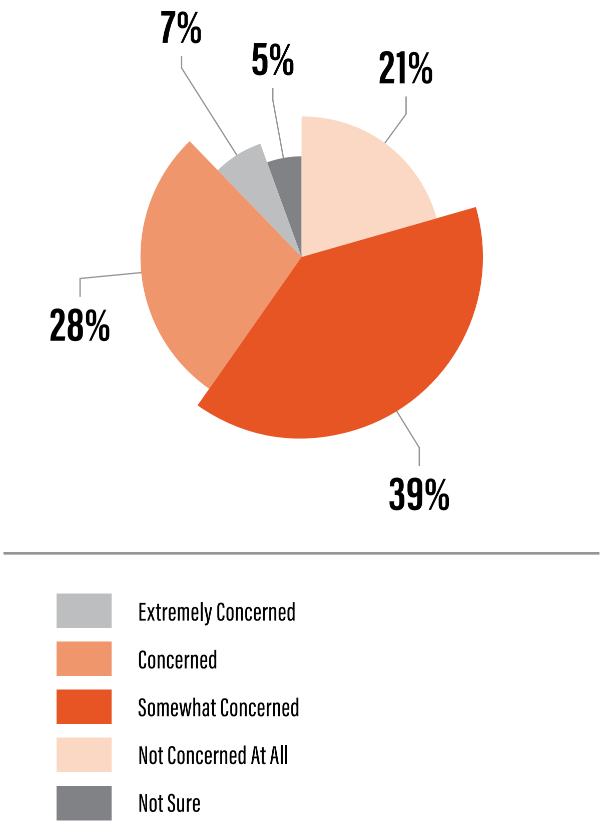
GRAPH 08 **DO YOU HAVE A BYOD POLICY IN PLACE?**



Number of respondents: **2017**—868; **2016**—330

Asadoorian, CEO of *Security Weekly*. "As a result, attackers are adapting and using mobile devices to pivot and attack IoT devices.[6] This is due, in large part, to the overall lack of protection on Android and IoT devices. The consequences are potentially disastrous as the new breed of IoT malware is being used for larger DDoS attacks, ransomware and distributing advertisements. More than ever before both BYOD and IoT security planning is crucial to an organization's security posture."

GRAPH 09 **HOW CONCERNED ARE YOU ABOUT THE THREAT OF UNAUTHORIZED PERSONAL MOBILE DEVICES, WEARABLE TECH, AND ACCESS POINTS TO YOUR NETWORK?**



Number of respondents: 868

While BYOD preparation has stalled, the number of devices coming into the office is growing all the time and posing new threats. 60% said they were concerned about the threat of unauthorized personal devices, wearable tech, and access points to their networks.

When asked about the possible compromise of devices in his office, one respondent said that "Odds are good we have had our devices hit but we don't have detection." Even standard devices like Netgear routers have vulnerabilities, without detection capabilities, IT Security is at risk to these exploits.[7] BYOD is a growing quagmire for IT security, as more than half of security professionals surveyed said they weren't sure when they had last checked devices employees bring into their offices OR had never checked at all.

Security professionals are uncomfortably aware that they may not have as much authority as they used to. 61% are concerned about Internet connected device purchases made without their knowledge, AND one-third of respondents who have a BYOD policy admit to having no way to enforce it—and those are the ones who will admit it.

Many companies have a BYOD policy that "is a policy on paper only." Only 30% have checked the devices employees bring into the office for malware in the last month. Equally important, as one of our respondents put it, is that even if there are good practices within one company, you have the problem of: *"Not in my company, but really concerned about my customers."*

BYOD: PERCEPTION | REALITY

While over half (55%) say that their organizations have a BYOD policy in place, a third of those respondents said they didn't have a way to enforce that policy (put another way, only 39% of respondents have both the policy and a way to enforce it). While that might not seem so bad, 42% of employee wireless devices had malware attacks in the last year and 40% never check for malware infections on the devices employees bring into the office. Looking past all the numbers we've mentioned, it is clear that employee devices are a significant attack surface in the enterprise into which security teams have little visibility.

CONCLUSION

THE FIRST STEP IN SOLVING A PROBLEM IS TO ADMIT THAT YOU HAVE ONE. IT IS CLEAR THAT INFOSEC PROFESSIONALS REALIZE THAT CONNECTED DEVICE THREATS POSE A SIGNIFICANT CHALLENGE. This isn't just a "cyber problem." It is a business, societal, and nation-state problem. Connected device attacks have proven they have the power to take down companies, damage economies, and shut down critical infrastructure.

The ultimate sign of change in 2017 and beyond will be found in security budgets. The number of respondents that have a budget or plan to have a budget for IoT security and BYOD security are up slightly.

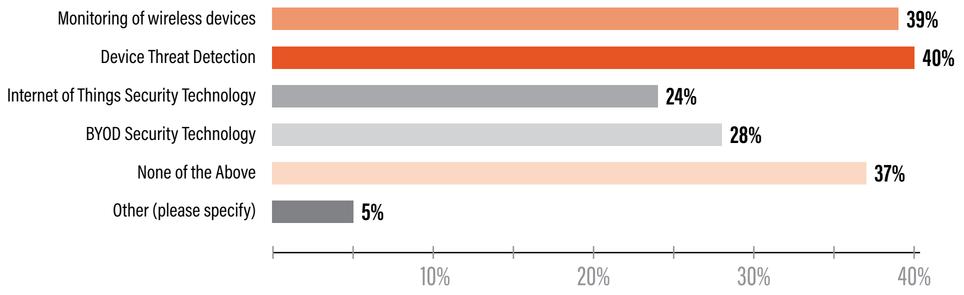
Before we declare that all is lost, abandon all hope, and no one can save the enterprise from rogue actors, one response gave us some hope that offices could be ready to make changes. More than half (54%) of respondents said that their companies would pay more for an IoT product that comes with extra or updated security provisions.

"We see innovators moving in the right direction across a range of industries—these devices are in a wide range of businesses across industries including financial services, hospitality, retail, manufacturing, professional services, technology, healthcare, energy and more," said Paul Paget. "The change agents are finding the funds to expose and address the device threats introduced by IoT and BYOD."

2016 kicked off with the DDoS attacks driven by the Mirai botnet, but 2017 will be the year of device-driven breaches. With Mirai and it's inspired offshoots in the wild, determined attackers see the potential to use vulnerable connected devices for nefarious large-scale purposes. The next step is using those same devices to compromise specific networks. In addition to attacks compromising our data security and efficiency, 2017 will be the year that physical security will start to be threatened by IoT.

While compromises of connected cars and power plant failures have happened in the past, we need to be concerned about connected physical security devices (locks, cameras, etc.) and connected

GRAPH 10 **OVER THE NEXT 6 MONTHS DO YOU HAVE A BUDGET IN PLACE OR CURRENTLY PLAN TO BUDGET FOR ANY OF THE FOLLOWING? CHECK ALL THAT APPLY.**



Number of respondents: 868

healthcare equipment. Even if these devices are not maliciously targeted, they can be compromised unintentionally by a user who accidentally connects them to another device with malware or an insecure network.

"If I've learned anything in the last two decades of fighting the good InfoSec fight, it's that we cannot protect systems unless we have a solid understanding of what is in our enterprise IT environments," said Aaron Turner. "Discovery and tracking of devices which are capable of bypassing traditional security controls will become ever more important as every little piece of electronics brings its own connectivity to the party."

With the world coming to the realization that these devices can cause serious harm, let's work together to ensure that the necessary investments are made to enable a secure connected future, rather than one driven by fear, uncertainty, and doubt.

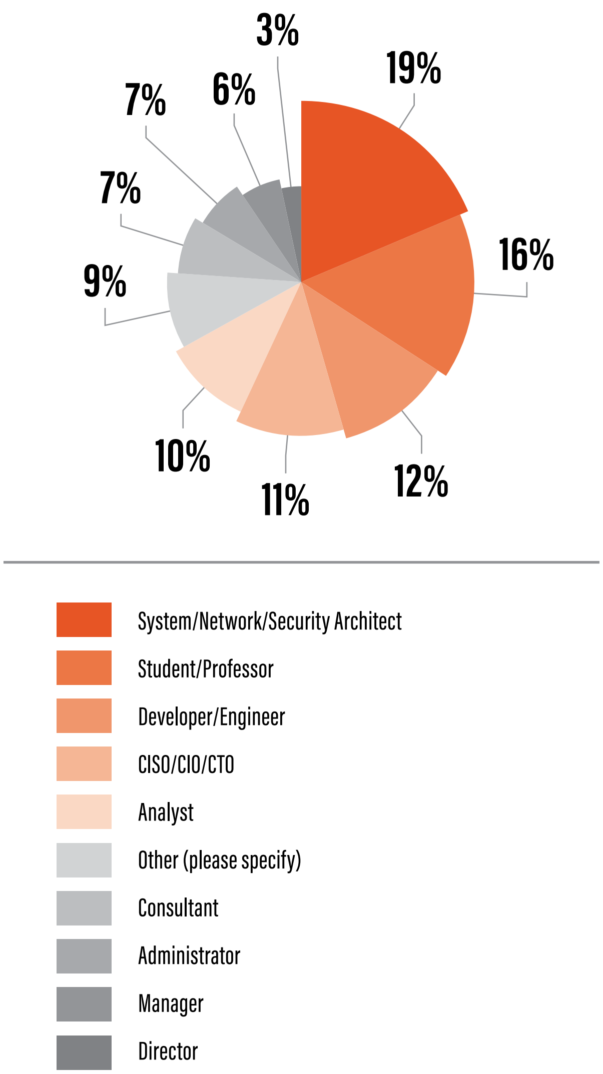
> "DISCOVERY AND TRACKING OF DEVICES WHICH ARE CAPABLE OF BYPASSING TRADITIONAL SECURITY CONTROLS WILL BECOME EVER MORE IMPORTANT AS EVERY LITTLE PIECE OF ELECTRONICS BRINGS ITS OWN CONNECTIVITY TO THE PARTY."
>
> —Aaron Turner, Independent IoT Security Researcher and Faculty at IANS

METHODOLOGY

WHO TOOK THE SURVEY?

950 people responded to at least one question from the Pwnie Express survey, with 868 completing all the questions. The margin of error of a survey with 800 respondents is roughly ±3%.[8]

GRAPH 11 **RESPONDENTS' TITLES IN THE WORKPLACE**

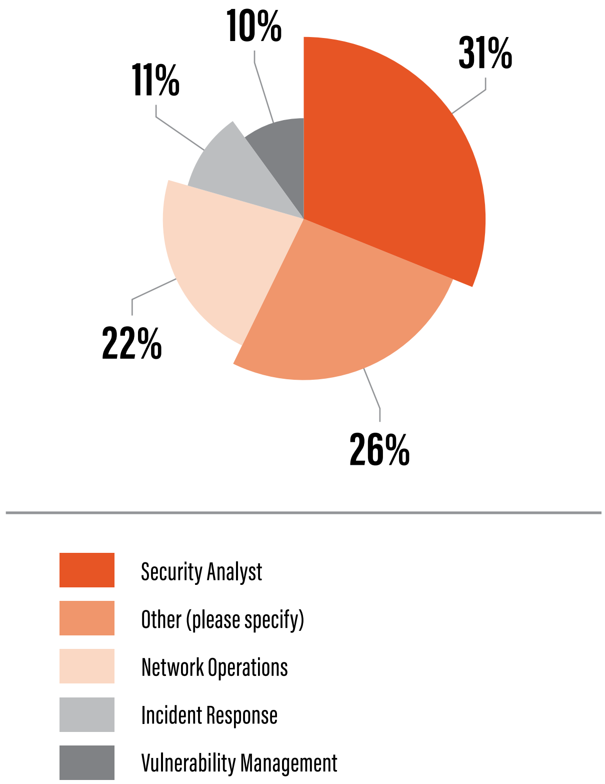


Number of respondents: 950

WHAT POSITIONS DO THEY HOLD?

Survey respondents included global InfoSec professionals, with positions ranging from CISOs, CIOs and CTOs to System Architects, Consultants and Analysts.

GRAPH 12 **RESPONDENTS' AREA OF EXPERTISE**



Number of respondents: 950

WHERE ARE THE RESPONDENTS FROM?

Most of the respondents said they were from the United States (639), followed by Canada (38), the United Kingdom (32), India (19), France (15), and Germany (14). Respondents from 80 countries took the survey.

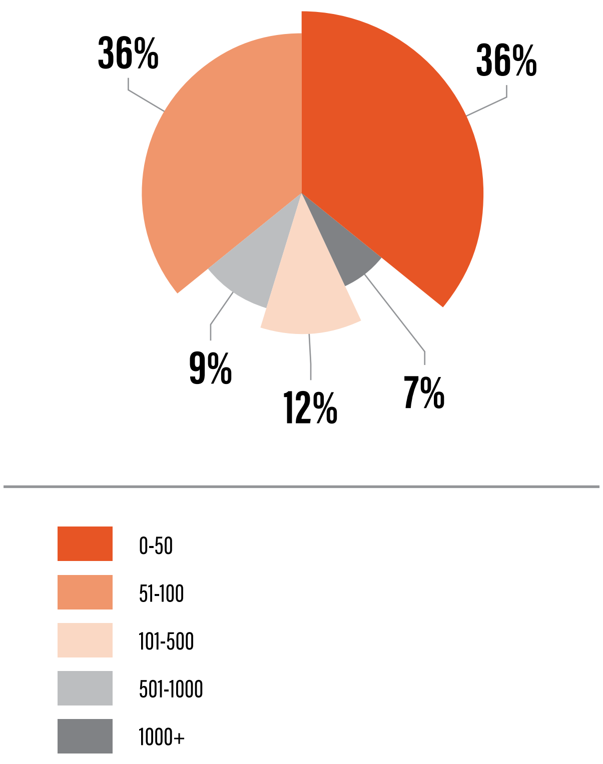
WHEN WAS THE SURVEY CONDUCTED?

Respondents answered Pwnie Express questions between December 14, 2016 to January 5, 2017.

HOW BIG ARE THE OFFICES IN WHICH THEY WORK?

We received responses from people working in different sized organizations, from smaller consulting groups to larger organizations.

GRAPH 13 **ABOUT HOW MANY EMPLOYEES DOES YOUR COMPANY HAVE?**



Number of respondents: 950

HOW DID THE RESPONDENTS GET THE QUESTIONS?

Respondents were contacted through our database by email and took the survey online from survey monkey. Some received the email directly from Pwnie Express and others were contacted through the Security Weekly mailing list.

Additionally, this report includes aggregate analysis of 86 million wired and wireless connections, network hosts and access points detected by Pwnie Express, using our proprietary wired, wireless, and Bluetooth assessment platform. The Pwnie Express Research team used the platform to assess certain threats posed by IoT devices. No personal or business information was compromised in the making of this report.

The analysis of the data was done in a manner consistent with the agreements Pwnie Express has with customers and data was used in aggregate only. Any PII was removed before processing.

The Pwnie Express research team more than doubled the number of questions in our online survey, doubled the number of survey respondents (from 400 last year to more than 800 for this report), and looked at more than 10 times the number of wireless devices, now up to 74.5 million compared to 7 million last year 1.48 million Set Service Identifiers[vi] (or SSIDs), and approximately 86 million connections from different kinds of devices, total.

[vi] SSID is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN). The SSID acts as a password when a mobile device tries to connect to the basic service set (BSS)—a component of the IEEE 802.11 WLAN architecture. (from www.webopedia.com/TERM/S/SSID.html)

ENDNOTES

[1] Woolf, Nicky. “Ddos Attack That Disrupted Internet Was Largest Of Its Kind In History, Experts Say”. the Guardian. 3 Nov. 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[2] Vincent, James. ”Don’t believe the story about hackers locking guests in their room at a luxury hotel.” The Verge. 30 Jan. 2017. http://www.theverge.com/2017/1/30/14438226/hackers-austrian-hotel-bitcoin-ransom-ransomware

[3] Alaybeyi, Saniye Burcu, Orans, Lawrence. “Real-Time Discovery, Visibility and Control Are Critical for IoT Security.” 3 Nov. 2016 https://www.gartner.com/doc/3500828/realtime-discovery-visibility-control-critical

[4] Phillips, Cassie. “Are Our Smartphones The New Attack Vector For Hackers?”. Blog Nokia Networks. 4 Jul. 2016. https://blog.networks.nokia.com/mobile-networks/2016/07/04/smartphones-new-attack-vector-hackers/

[5] Mimoso, Michael. “FBI Mum On Real-World Keysweeper Attacks”. Threatpost | The first stop for security news. 24 May 2016. https://threatpost.com/fbi-mum-on-real-world-keysweeper-attacks/118260/

[6] Buchka, Nikita “Switcher: Android Joins The ‘Attack-The-Router’ Club—Securelist”. Securelist.com. 28 Dec. 2016. https://securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/

[7] Brooke, Chris. “Hundreds of Thousands of Netgear Routers Vulnerable to Password Bypass.” Threatpost.com. 30 Jan, 2017. https://threatpost.com/hundreds-of-thousands-of-netgear-routers-vulnerable-to-password-bypass/123462/

[8] https://www.isixsigma.com/tools-templates/sampling-data/margin-error-and-confidence-levels-made-simple/

DETECT, ASSESS, AND RESPOND TO BYOD AND IOT DEVICE THREATS

Pwnie Express addresses the attack surface exposed by BYOD, IoT, and connected devices in the enterprise. By continuously discovering, monitoring and assessing all devices on and around a company's network, Pwnie Express provides security professionals the ability to detect, assess, and respond to device based threats, including misconfigured, unauthorized, and malicious devices.

With our easy to deploy and operate SaaS platform, Pulse, Pwnie Express makes it easy for security teams to:

- Automatically discover, fingerprint and track all devices on and around your network and classify their trust level.
- Continuously analyze device configurations and behavior, and identify high risk interactions between trusted and non-trusted devices or networks.
- Minimize risk and exposure to attack through threat discovery, classification, and alerting to defeat attacks earlier in the kill chain.

TO LEARN MORE ABOUT PWNIE EXPRESS VISIT WWW.PWNIEEXPRESS.COM.

Pwnie Express   Pwnie Express   @PwnieExpress

268 SUMMER STREET, FLOOR 2 • BOSTON, MA 02210 • T: (855) 793-1337 • F: (857) 263-8188