WHO IS WATCHING YOU?

WHO IS WATCHING OUT FOR YOU?

2018

THE INTERNET OF EVIL THINGS®

PWNIE EXPRESS

@PwnieExpress

TABLE OF CONTENTS

TABLE OF GRAPHS

EXECUTIVE SUMMARY

The 2018 Pwnie Express Internet of Evil Things® survey results are in.

For the fourth consecutive year, we polled hundreds of information security professionals to get a detailed look at their perceptions, awareness and preparedness for cyberattacks on their organizations.

As you will see, security professionals are more concerned than ever about what they see as the growing threat.

In fact, 85 percent believe their country will suffer a major cyberattack on its critical infrastructure in the next five years, in almost any given category (i.e., healthcare, energy, or transportation to name just a few.)

As compared to a year ago, 64 percent of respondents are more concerned about connected device threats, with IoT devices at the top of the list. Yet, slightly fewer are checking their wireless devices than last year. And one in three report that their organizations are unprepared to detect connected device threats.

Other key report findings include:

- Malware is the largest threat, with nearly 60 percent of organizations suffering from a malware attack in 2017.
- Employee-owned devices (otherwise known as BYOD) are a concern for 80 percent of our respondents, yet fewer than 50 percent can monitor BYODs in real time.
- As in last year's report, small-to medium-sized organizations (SMOs) continue to be surprisingly more vigilant than larger enterprises. Just 49 percent of organizations with more than 1,000 employees know how many devices are connected to their networks as compared to 70 percent of SMOs.
- Security professionals believe that the biggest impact of a cyberattack on their organization would be negative brand perception.
- The majority of security professionals feel they are most responsible for connected device security, yet they are often left out of device purchasing decisions.
- Most organizations need to update their security policy to include IoT devices. Many are two times as likely to have an IT versus IoT policy.

In addition to the top five threats detailed in the report, in 2017 we also saw the scope of attacks expanding. For example, the attack on a Schneider Electric safety system was designed to sabotage an industrial plant and cause bodily harm to workers.

Perhaps that is why we are seeing the federal government begin to take steps that would help shift accountability to manufacturers of IoT devices. However, our report reveals that security professionals are split on whether they would welcome such involvement.

In conclusion, 2018 marks the fourth consecutive year where perceptions and awareness of cyberattacks outpace prevention and action. Despite recent high-profile attacks, we are concerned that a "head in the sand" strategy continues to reign. We fear that those organizations not making the necessary cyber security investments won't be able to hide forever.

1. EVIL ON THE INCREASE

THE SCARIEST SURVEY RESULTS WE'VE SEEN YET

Security professionals have spoken. The 2018 Pwnie Express Internet of Evil Things® survey results are in and they do not paint a pretty picture. As you will see, by almost every measure, the rate and severity of cyberattacks have increased in 2018. What's worse, the scope of attacks has broadened.

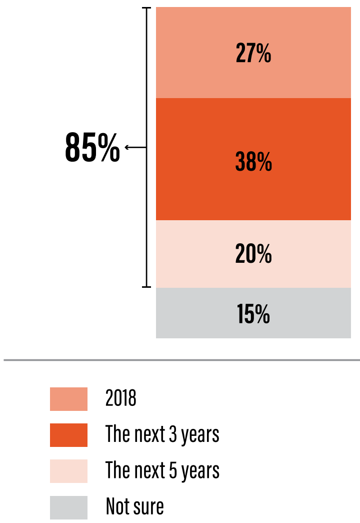
As we saw in the news, not only are traditional corporate IT breaches of confidential data occurring, but new classes of threats are emerging. For example:

> *The attack on a Schneider Electric safety system was considered a watershed moment because it demonstrated how hackers "might cause physical damage to a plant, or even kill people by sabotaging safety systems before attacking industrial plants."*[1]
>
> *The US-CERT alerted Americans to a "multi-stage intrusion campaign by the Russian government to spear phish and gain remote access into energy sector networks."*[2]

Given the above, it is not surprising that the more than 500 security professionals who took this year's Internet of Evil Things® survey see the potential for even larger, more devastating attacks.

In perhaps what is the most stark finding we've seen in the four years since we began polling security professionals—85 percent think their country will suffer a major cyberattack on its critical infrastructure in the next five years.

GRAPH 01 DO YOU THINK THAT YOUR COUNTRY WILL SUFFER A MAJOR CYBERATTACK ON ITS CRITICAL INFRASTRUCTURE IN:



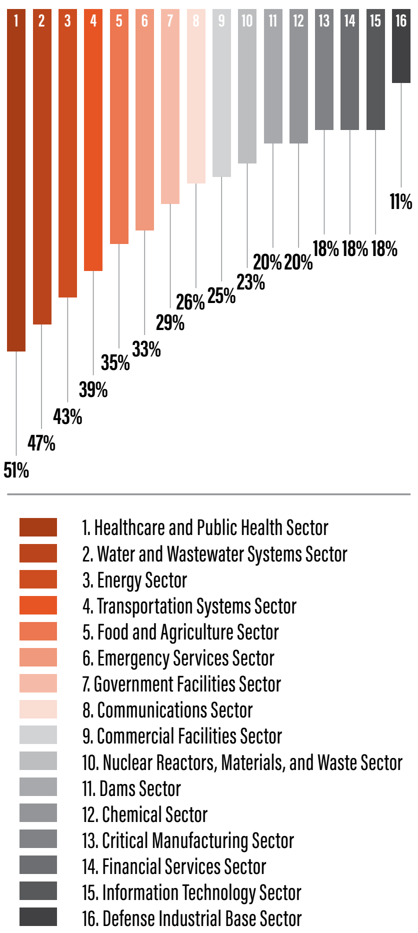
No. of respondents: 579

Our next question dug deeper into which specific infrastructure categories security professionals believe are least prepared for such attacks. The graph to the right shows that more than half of the 500-plus respondents said the healthcare and the public health sectors were the least prepared for a cyberattack. 47 percent included the waste and wastewater sectors on that list, and another 43 percent said the energy sector was amongst the least prepared.

While concerns about the healthcare sector top the list, what strikes us about this graph is that 3/4ths of the categories received 20 percent or greater distribution.

And when we synthesize the responses to these two questions, we can't help but come to a troubling conclusion: **A cyberattack on critical infrastructure is most certainly on the horizon… and it could happen in almost any category.**

GRAPH 02 WHAT CRITICAL INFRASTRUCTURE CATEGORIES ARE LEAST PREPARED FOR CYBERATTACKS?*



No. of respondents: 558

*Respondent could make up to three selections for this question.

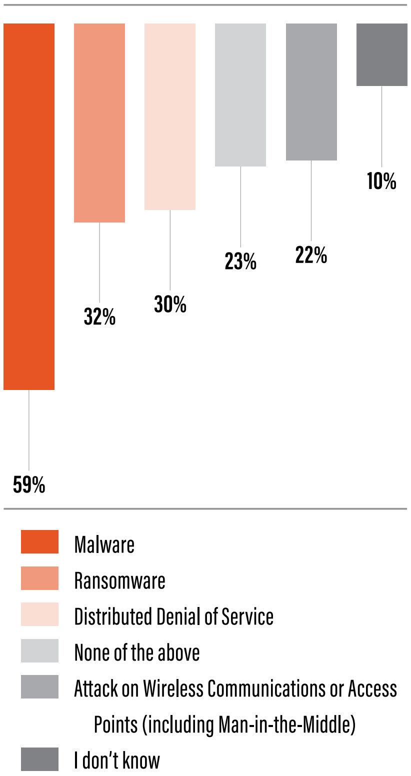
2. THE TOP FIVE THREATS

EVALUATING MALWARE AND VULNERABILITIES

Security professionals battled with plenty of malware (59 percent) and ransomware (32 percent) this year. Additionally, almost one-third of our respondents reported fighting off Distributed Denial of Services (DDoS) attacks, many of which are fueled by IoT botnets, and more than 22 percent discovered attacks on wireless communications or access points (that includes Man-in-the-Middle attacks.)

When we dug deeper, five percent of respondents experienced MitM attacks last year.

GRAPH 03 WHAT CATEGORY OF ATTACKS HAS YOUR ORGANIZATION EXPERIENCED IN THE PAST YEAR?



No. of respondents: 579

A DETAILED LOOK AT THE WORST FIVE EVENTS

MIRAI

Mirai is a malware that targets online consumer devices such as IP cameras and home routers. The infected machines are turned into remotely controlled bots that are used for large-scale DDoS network attacks.

At the end of 2016, McAfee Labs estimated Mirai infected 2.5 million IoT devices. Every minute, another five IoT device IP addresses were added to the Mirai botnet armies.[3] For example, 80 camera models manufactured by Sony were vulnerable to a Mirai takeover.[4]

This year, only 11 percent of our respondents reported being affected by Mirai, however more than 40 percent of respondents said they either were not or did not know if they were any better prepared to deal with Mirai than they were at this time last year. Perhaps that's why we are seeing new strains of Mirai. In the early part of 2018, Fortinet found the "OMG" variant of Mirai which "infected devices to act as proxy servers capable of protecting the anonymity of cybercriminals engaging in illegal activities."[5] Recorded Future's research arm, the Insikt Group, found a Mirai variant that had attacked at least one financial services company.[6] With the code easily available and tens of millions of vulnerable IoT devices being sold, as long as companies can't detect Mirai, it will continue to be a popular weapon for threat actors.

WANNACRY

WannaCry is a ransomware cryptoworm propagated through Windows machines.[7] In 2017, about 200,000 computers across more than 150 countries were affected, with the biggest impact being felt in the National Health Services in England and Scotland.[8] In addition to the general issues of computers being locked, healthcare devices were also frozen. MRI scanners, blood storage refrigerators, and other medical equipment were compromised to the point that non-critical patients were turned away from some facilities.[9]

According to our respondents, WannaCry seems to be most dangerous for certain types of organizations—larger healthcare and technology organizations—the specific target of the above attacks. Also of concern was that government respondents were least likely to know if they had been affected by WannaCry.

While 21 percent of our participants said they experienced WannaCry attacks last year, about 18 percent said they didn't have the tools to address WannaCry, with about 14 percent responding that they did not know if they did.

NOTPETYA

NotPetya is another ransomware cryptoworm that has taken down more than just home computers. Potentially politically motivated, the worm was responsible for a swath of attacks across the world, hitting companies and organizations in Ukraine the hardest, as well as, the U.S, the U.K., Germany, Poland, Italy, France, and Russia.[10] On the corporate level, NotPetya took down the major shipping company, Maersk, which lost somewhere in the range of $200—$300 million in revenue from the attack.

In this year's survey, 10 percent of security professionals said they experienced NotPetya attacks and an additional 13 percent were not sure whether or not they had. When asked if they had the tools to detect a NotPetya attack, 37 percent either did not have the tools or had no clue if they did.

In this case, the math tells an alarming story. 77 percent of security professionals said they had NOT experienced a NotPetya ransomware attack in the past year. However, only 63 percent said they had the tools necessary to detect such an attack. That 14 percent gap is cause for concern that this may be a case of overconfidence in security or under reporting of NotPetya attacks.[11]

LOCKY

Locky, an older ransomware malware, is nevertheless still causing damage wherever it rears its ugly head. The software seems to be the work of a semi-professional group who initially released it in 2016, and then re-released it with updates in 2017.[12] In February 2016, Hollywood Presbyterian Medical Center in Los Angeles was affected, and the staff was locked out of computers and electronic records.[13]

Twelve percent of our respondents were affected by Locky in the last year. One of the biggest issues with Locky are the variants—it's hard to know if it will be back. Unfortunately, 20 percent of those surveyed said they didn't have the tools to deal with the threat, and another 19 percent didn't know (39 percent total) if they did.

KRACK

KRACK is a very serious attack on WPA2, which has been widely considered a secure form of wireless.[14] While there have been patches released for the vulnerability, they are not yet very widely implemented. Microsoft recently applied a patch associated with KRACK, but it seems as though the community is still grappling with the implications of the vulnerability.[15]

KRACK works against "all modern protected networks" and, concerningly, is Operating System agnostic.[16] The attacker needs to be in WiFi range of the susceptible device. Huge amounts of sensitive data pass through routers every day, and KRACK makes this all susceptible, particularly if the user is unaware of any suspicious devices in the physical area around the access point.

Overall, 10 percent of our respondents experienced a KRACK attack, while an additional 17 percent didn't know if they had been affected, leaving 73 percent who said they were unaffected by KRACK. A closer look at the numbers, however, reveals cause for concern as 24 percent admitted they don't have the tools to detect KRACK and another 22 percent don't know if they do. These numbers beg the question: How can 73 percent of security professionals say they haven't been affected by a vulnerability when only 54 percent of them have the tools necessary to detect it?

3. LITTLE OR NO IMPROVEMENT IN DEVICE SECURITY

STRESS AND UNEASE IN THE IOT SECURITY COMMUNITY, BUT NOT MUCH ACTION

Not surprisingly, as the number of threats continue to grow, concern about device security is sky-rocketing.

Sixty-four percent of our respondents said they are more worried about device threats than they were at the same time last year.

The following table uses open-ended data, derived through multiple choice questions posed to our pool of security professionals, and helped us to gain perspective on their leading areas of concern:

Increase in multitude and variety of devices	100	16%
Hackers advancing, increases in targeted attacks	74	12%
Lack of security in device manufacturing	70	11%
Increase in IoT	51	8%
Increased network connectivity	45	7%

(see Appendix A for full table)

We then asked open-ended questions about what types of devices posed a threat and Internet of Things was at the top of the list:

IoT	82	18%
Mobile/Smartphone	59	13%
BYOD (Bring Your Own Device)	42	9%
Purpose built malicious devices	41	9%
Rogue Devices	25	6%

(see Appendix B for full table)

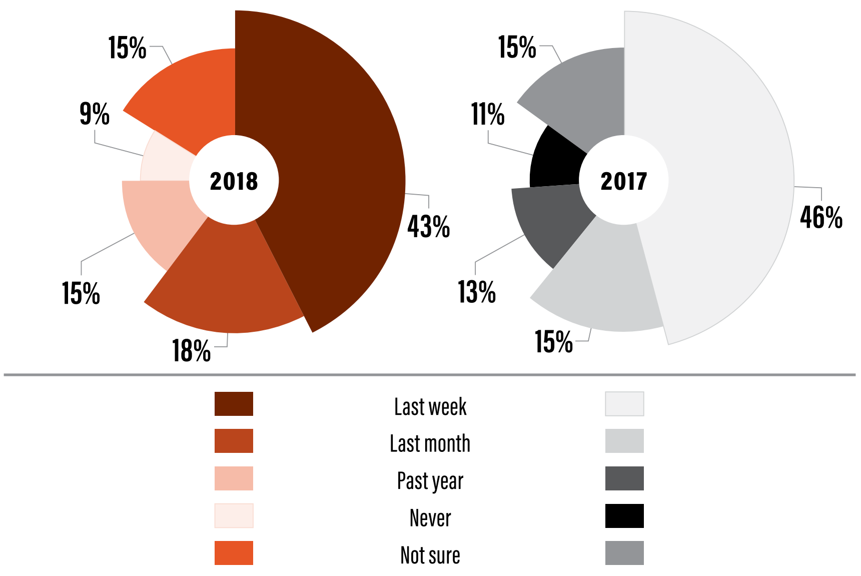
This result is particularly troubling for us at Pwnie because we well understand the dangers posed by connected IoT devices.

And, security professionals repeatedly reported that connected devices pose threats they cannot adequately address. Consider that:

- **One in three** respondents said that their organizations were unprepared to detect connected device threats.
- **49 percent** are concerned about consumer IoT devices like smart watches, smart coffee-makers, and the like while only **23 percent** can monitor for these types of devices.
- **80 percent** are concerned about BYOD devices in the workplace but only **47 percent** can monitor for them in real time.
- **51 percent** are concerned with malicious or purpose-built rogue devices, but only **24 percent** can monitor for them in real time.

Despite these concerns, when we compared this year's findings to some of our questions from 2017's survey, the frequency with which respondents are checking their wireless devices showed no improvement (and in fact had decreased slightly).

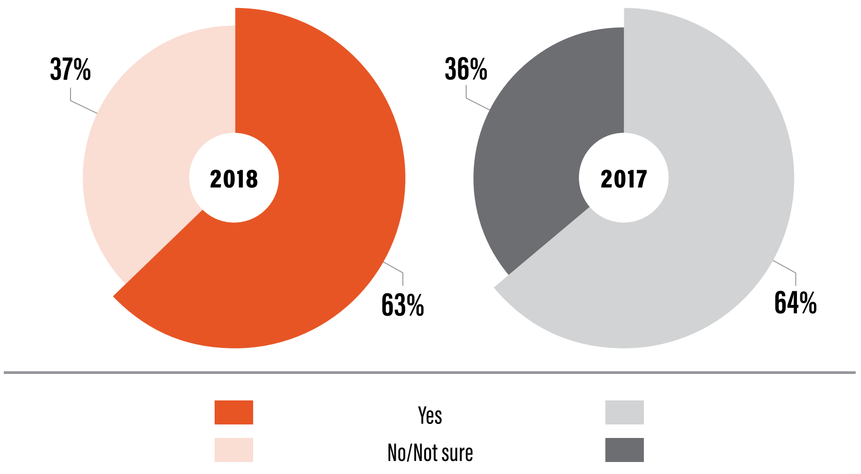
GRAPH 04 WHEN WAS THE LAST TIME YOU CHECKED YOUR WIRELESS DEVICES FOR MALICIOUS INFECTIONS?



No. of respondents 2018: 592; No. of respondents 2017: 868

Similarly, when we asked, "Is the detection and mitigation of rogue, unauthorized and malicious devices a high priority for your security program today?", we again saw no improvement (and in fact a slight decrease).

GRAPH 05 IS THE DETECTION AND MITIGATION OF ROGUE, UNAUTHORIZED AND MALICIOUS DEVICES A HIGH PRIORITY FOR YOUR SECURITY PROGRAM TODAY?



No. of respondents 2018: 592; No. of respondents 2017: 868

In conclusion, while 64 percent of respondents are more concerned about security threats to connected devices than last year, they are reporting no improvement in the frequency with which they are checking them. In fact, they are checking these devices with slightly less frequency and detection and mitigation is slightly lower on their program's priority scale. We believe this is cause for concern.

4. SIZE MATTERS

SMOs STUNNED US LAST YEAR. HAS ANYTHING CHANGED?

For last year's IoET survey, Pwnie researchers wanted to see how organizations of varying sizes were handling the security challenges posed by IoT devices. Interestingly, our findings indicated that while small & mid-sized organizations (SMOs) have fewer resources than their larger counterparts, they generally demonstrate better security practices than the larger organizations we surveyed. For example:

- SMOs had more knowledge of how many devices are connected to their network (**62% to 47%**).
- SMOs were more likely to make monthly checks of their wireless devices for malicious infection (**64% to 55%**).
- SMOs were more likely to have knowledge of how many connected devices their employees are bringing into work (**39% to 25%**).
- SMOs were more likely to make monthly checks of devices employees bring into the office for malicious infections in the last month (**33% to 20%**).

Fast forward to the here and now and Pwnie's researchers again asked organizations of varying sizes how often they check devices. We also asked what types of threats the Internet of Evil Things is confronting SMOs with in comparison to larger ones.

We found that larger organizations experienced attacks at higher rates in several key categories including distributed denial of service (DDoS), ransomware, and malware. Malware attacks, in particular, were experienced by an astounding 71 percent of large organizations.

WHAT CATEGORY OF ATTACKS HAS YOUR ORGANIZATION EXPERIENCED IN THE LAST YEAR?

	1-1000	**1000+**
DDoS	**26%**	**38%**
Ransomware	**25%**	**45%**
Malware	**53%**	**71%**
WCs or APs	**21%**	**23%**

Similarly, in the case of specific attacks by WannaCry, NotPetya and Locky, larger organizations experienced attacks at a ratio of nearly 2 to 1 compared to SMOs.

DID THIS TYPE OF ATTACK IMPACT YOUR ORGANIZATION IN THE LAST YEAR?

	1-1000	**1000+**
WannaCry	**17%**	**34%**
NotPetya	**8%**	**20%**
Locky	**9%**	**16%**

In spite of this, tor the second year in a row, SMOs outpaced their larger counterparts with 68 percent checking their wireless devices in the last month, compared to only 49 percent for large organizations.

WHEN WAS THE LAST TIME YOU CHECKED YOUR WIRELESS DEVICES FOR MALICIOUS INFECTIONS OR KNOWN VULNERABILITIES?

	1-1000	1000+
Last Week	48%	34%
Last Month	20%	14%
Total	68%	49%

Researchers found even more cause for concern when barely 1 in 2 large organizations responded that they know how many devices are connected to their networks, compared to over 70 percent for SMOs.

DO YOU KNOW HOW MANY DEVICES ARE CONNECTED TO YOUR NETWORK?

	1-1000	1000+
Yes	71%	49%

Worse still, an alarming number of organizations of all sizes, but especially large organizations, believe that there are connected devices on their network of which they are unaware.

DO YOU THINK THERE ARE CONNECTED DEVICES ON YOUR NETWORK THAT YOU ARE UNAWARE OF?

	1-1000	1000+
Yes	46%	71%

Overall, the results of this year's deeper dive into the comparison of IoET challenges and practices at SMOs and large organizations reveals a troubling trend. While larger organizations face more attacks in several key categories, SMOs remain more vigilant as compared to their larger counterparts.

5. MANAGEMENT BEST PRACTICES

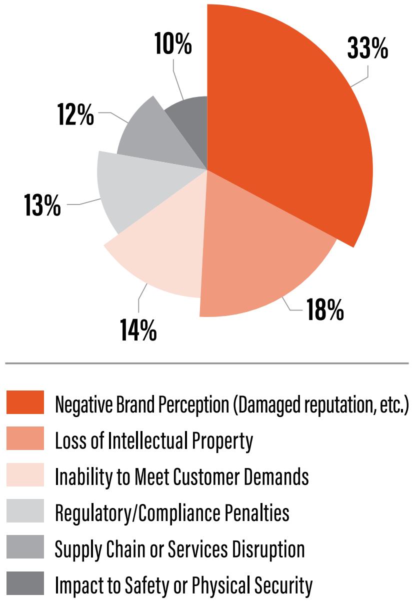
KEY TAKEAWAYS FOR REDUCING THE THREAT

POOR SECURITY THREATENS YOUR ORGANIZATION'S BRAND

For years, we've heard the refrain that cybersecurity is a sunk cost—as if there's no return for good cyber hygiene. Now, as more high-profile organizations experience the backlash from customers who learn of a breach (think Target or Equifax), this perception is changing—as it should.

When we asked the security pros what the biggest impact would be of a cyberattack on their organization, a third of all respondents answered, "negative brand perception." No other choice got to 20 percent.

GRAPH 06 WHAT DO YOU FEAR WOULD BE THE BIGGEST IMPACT OF A CYBERATTACK ON YOUR ORGANIZATION?



No. of respondents: 626

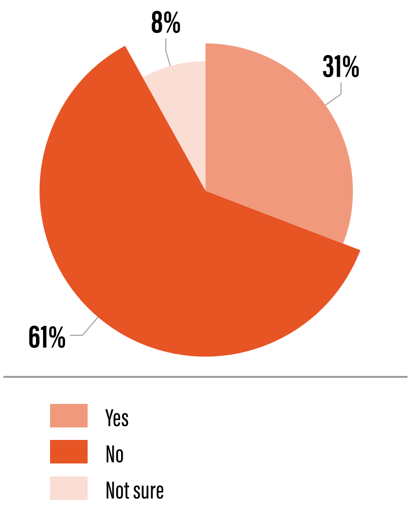
SECURITY PROS NEED TO BE INVOLVED IN PURCHASING DECISIONS

It seems like common sense that the experts should be consulted when device purchases are made. However, our data shows that your security pros are left out of the purchasing and clearance process as much as two-thirds of the time.

Furthermore, size of organization was not a factor. In fact, larger revenue producing companies are not as good at clearing device purchases as smaller ones (see Graph 08 below).

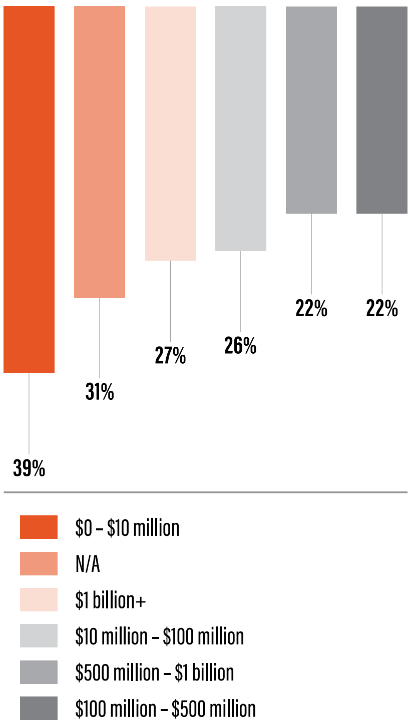
We were even more dismayed when we looked at the numbers by product area and learned that in three vulnerable categories—Building OT/IoT, Industrial IoT, and Consumer IoT—less than 50 percent of security professionals are involved in the purchasing approval process.

GRAPH 07 DO ALL DEVICE PURCHASES HAVE TO BE CLEARED BY SECURITY PERSONNEL?



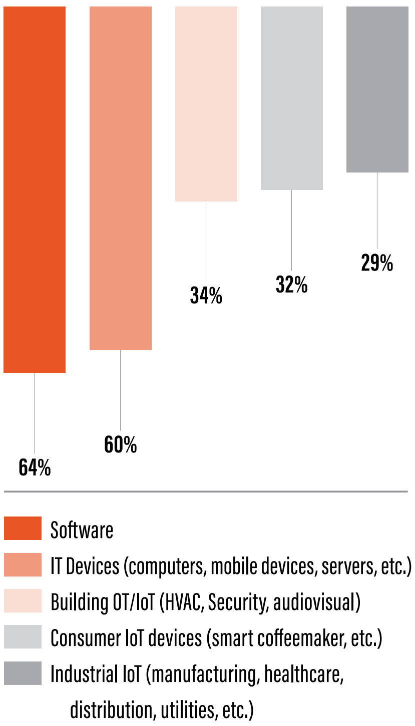
No. of respondents: 592

GRAPH 08 ORGANIZATIONS WHERE DEVICE PURCHASES ARE CLEARED BY SECURITY PERSONNEL (BY REVENUE)



No. of respondents: 592

GRAPH 09 DO YOU HAVE A ROLE IN THE PURCHASING APPROVAL PROCESS FOR THE FOLLOWING TECHNOLOGY PRODUCTS? (ANSWERED: I AM INVOLVED)



No. of respondents: 592

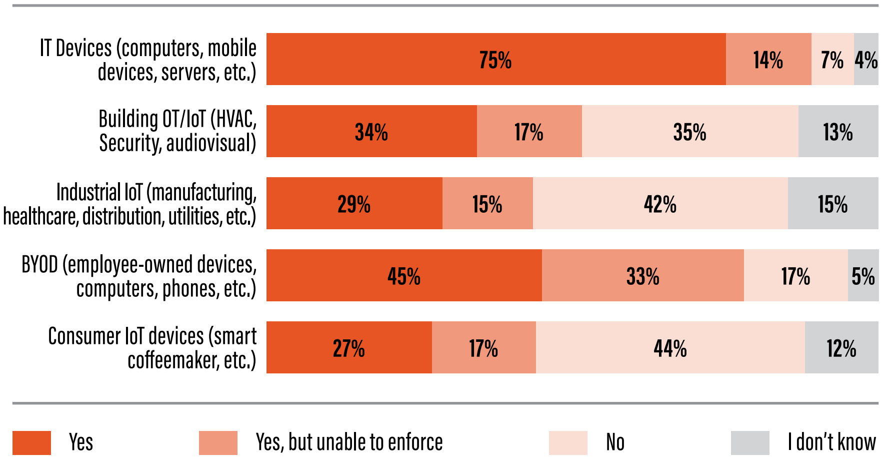
UPDATE SECURITY POLICY TO INCLUDE IOT DEVICES

Many of the security pros we talked with said their employers were **more than two times as likely** to have an enforceable security policy in place for IT devices than for IoT.

In the case that a security policy is in place, only a little more than one-third of security pros said that they themselves are involved in checking that ANY devices are compliant.

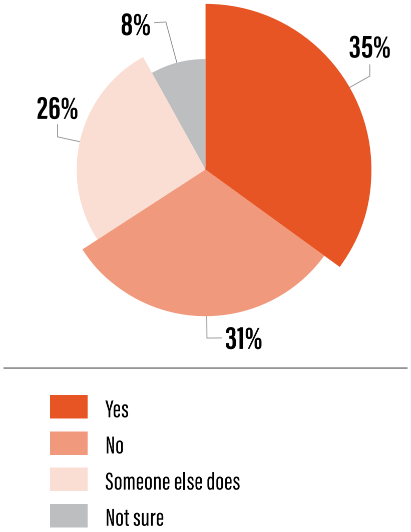
About 40 percent of respondents said either they didn't ensure devices were compliant or they were not sure that anyone in their organization does check.

GRAPH 10 DO YOU HAVE A SECURITY POLICY IN PLACE FOR THESE TYPES OF DEVICES?



No. of respondents: 592

GRAPH 11 DO YOU ENSURE THAT ANY DEVICES THAT ARE PURCHASED ARE COMPLIANT WITH ORGANIZATION SECURITY POLICIES?



No. of respondents: 592

6. WHO IS RESPONSIBLE?

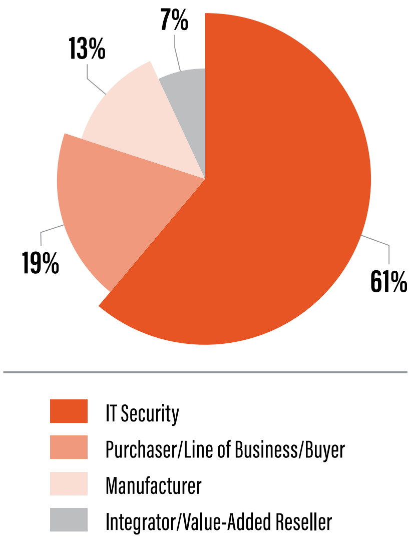
A MATTER OF OPINION

When we asked security pros who is responsible for connected device security, **the majority (60+%) of our survey participants believe that they (IT Security) shoulder most of the responsibility**. Interestingly, only 13 percent felt the device manufacturer was most responsible.

The U.S. government may have a different idea. Congress is beginning to take steps that would help shift more accountability to manufacturers of IoT devices. Several legislators have introduced bills, including The Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (by Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines), which would create disclosure guidelines for vendors selling IoT to the U.S. government.[17] The Cyber Shield Act (by Senator Ed Markey and Congressman Ted Lieu) would establish a voluntary cybersecurity certification program for IoT devices, which would enable manufacturers to certify that their product meets certain cybersecurity and data security benchmarks, and display this certification to the public.[18]

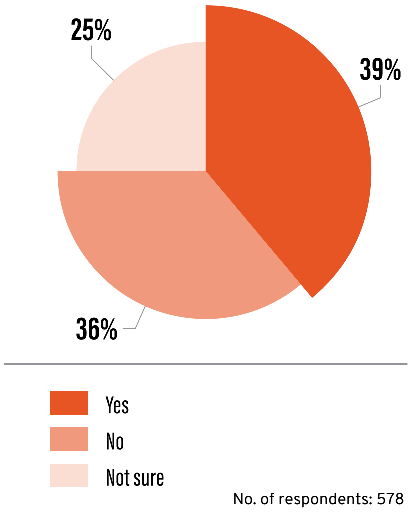
However security professionals are fairly split when it comes to whether the government should take a more active role in regulating security of IoT devices, as Graph 13 shows.

GRAPH 12 WHO IS MOST RESPONSIBLE FOR CONNECTED DEVICE SECURITY? (IOT IP CAMERAS, HVAC SYSTEM, MEDICAL DEVICES, ETC.)



No. of respondents: 586

GRAPH 13 SHOULD THE GOVERNMENT REGULATE SECURITY STANDARDS OF IOT DEVICES?



No. of respondents: 578

METHODOLOGY FAQ

WHO TOOK THE SURVEY?

A total of 708 people responded to the Pwnie Express survey. The margin of error in a survey with 500 respondents is roughly ±4 percent.[19]

WHAT POSITIONS DO THEY HOLD?

Survey respondents included global InfoSec professionals, with positions ranging from IT Management to Directors and VPs of IT and Security, Executive Management, Managers, Administrators to Consultants, Developers, Engineers, Professors and Students.

WHERE ARE THE RESPONDENTS FROM?

Most of the respondents said they were from the United States (494), followed by Canada (26), the United Kingdom (21), Australia (15) and India (12). Respondents from 57 countries took the survey.

WHEN WAS THE SURVEY CONDUCTED?

Respondents answered Pwnie Express questions between January 8 and March 5, 2018.

HOW BIG ARE THE OFFICES IN WHICH THEY WORK?

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

HOW DID THE RESPONDENTS GET THE QUESTIONS?

Respondents were contacted via email between January 8 to February 27, 2018 and invited to the online survey hosted by SurveyMonkey. The respondents provided their emails to Pwnie Express and agreed to have them stored in the company's database when they subscribed for Pwnie's monthly newsletter. The survey link was sent directly from Pwnie Express. A link to the survey was also posted on Pwnie's twitter page where potential respondents could share their answers.

APPENDIX A

If you answered “Yes” on #9 (Are you more worried about device threats than you were 12 months ago?), please answer why:

Increase in multitude and variety of devices	100	15.75%
Hackers advancing, increases in targeted attacks	74	11.65%
Lack of security in device manufacturing	70	11.02%
Increase in IoT	51	8.03%
Increase network connectivity	45	7.09%
Increase in BYOD and Personal Devices	35	5.51%
I became more aware	34	5.35%
Increase in vulnerabilities	31	4.88%
Human error/lack of education on security	29	4.57%
Lack of patching and updates	23	3.62%
The Unknowns	19	2.99%
Bigger Targets (Equifax, DHS, etc.)	15	2.36%
Lack of control	12	1.89%
Media Coverage exposing vulnerabilities	12	1.89%
Hardware Threats	11	1.73%
Threat actors	8	1.26%
No/poor strategy in place	8	1.26%
Increase in Ransomware	8	1.26%
Constant Change	6	0.94%
Lack of visibility	6	0.94%
Speed of Attacks	5	0.79%
Increase of Personal and sensitive information through devices	4	0.63%
Open Networks	4	0.63%
More Apps	4	0.63%
Zero Day Exploits	4	0.63%
Default Passwords	3	0.47%
NSA	3	0.47%
Pivot Point	2	0.31%
Android	2	0.31%
Man-in-the-Middle	2	0.31%
Shadow IT	2	0.31%
Yegen	1	0.16%
PV6	1	0.16%
Increase in Cloud usage	1	0.16%
Open source Code	1	0.22%
Door Locks	1	0.22%
Power Grid	1	0.22%
EDL Mandate	1	0.22%
Software exploits	1	0.22%
Intel Chip	1	0.22%
Printers	1	0.22%
Keyloggers	1	0.22%
RFID cloners	1	0.22%
Linux	1	0.22%
Passwords	1	0.22%
Megazord	1	0.22%
Refrigerators	1	0.22%
Apps	1	0.22%

APPENDIX B

What new device or types of devices are you worried about threatening your organization?

IoT	82	18.18%
Mobile/Smartphone	59	13.08%
BYOD	42	9.31%
Purpose built malicious devices	41	9.09%
Rogue Devices	25	5.54%
Unknown/unauthorized Devices	25	5.54%
Wearables	21	4.66%
WiFi/Wireless	18	3.99%
Laptops	14	3.10%
TVs	11	2.44%
USB, Plug in devices	11	2.44%
Video, camera, microphone devices	10	2.22%
People	7	1.55%
Raspi	7	1.55%
Bluetooth	6	1.33%
Android	6	1.33%
Alexa, etc.	6	1.33%
3rd party devices (vendors, server providers)	5	1.11%
Pineapple	5	1.11%
Drones	4	0.89%
Smarthome	4	0.89%
Sniffing devices	3	0.67%
HVAC	3	0.67%
AI	3	0.67%
Industrial	2	0.44%
Man-in-the-Middle	2	0.44%
Outdated infrastructure	2	0.44%
Servers	2	0.44%
Windows	2	0.44%
Zigbee	2	0.44%
Cars	2	0.44%
Lab Equipment	2	0.44%
Pwn Phone	2	0.44%
Chinese Devices	1	0.22%
Open source Code	1	0.22%
Door Locks	1	0.22%
Power Grid	1	0.22%
EDL Mandate	1	0.22%
Software exploits	1	0.22%
Intel Chip	1	0.22%
Printers	1	0.22%
Keyloggers	1	0.22%
RFID cloners	1	0.22%
Linux	1	0.22%
Passwords	1	0.22%
Megazord	1	0.22%
Refrigerators	1	0.22%
Apps	1	0.22%

APPENDIX C

What is it about connected devices and IoT that you are most worried about threatening your organization?

Bad Security	71	14.92%
Inability to Track/Control	51	10.71%
No Standards/Regulation	44	9.24%
Exposure	38	7.98%
Malware Spread	30	6.30%
Remote/Open/Unauthorized Access	30	6.30%
Lack of Patches/Updates	28	5.88%
The Unknowns	27	5.67%
Multitude/Variety	22	4.62%
Bad Actors/Enemy States	16	3.36%
Pivoting	13	2.73%
Smartphones	13	2.73%
Data Loss	11	2.31%
DDOS Attacks	10	2.10%
WiFi Sharing	8	1.68%
Snooping/Sniffing/Spying	7	1.47%
People	7	1.47%
Camera+Listening Capabilities	7	1.47%
Botnets	7	1.47%
Shared/Global Passwords	5	1.05%
IoT	4	0.84%
Smart TV	3	0.63%
Devices Are Always On	3	0.63%
Pwn/Pwn Phone	3	0.63%
BYOD	3	0.63%
Tablets/Laptops	2	0.42%
External Hard Drives	2	0.42%
Zombie Devices	2	0.42%
Crypto Mining	2	0.42%
AI Devices	1	0.21%
Bricking Systems	1	0.21%
Scada Sensors	1	0.21%
HVAC	1	0.21%
Chinese Devices	1	0.21%
Raspi	1	0.21%
Smart Home	1	0.21%

ENDNOTES

[1] Finkle, Jim. “Schneider Electric says bug in its technology exploited in hack.” Reuters. 18 Jan. 2018. https://ca.reuters.com/article/technologyNews/idCAKBN1F7228-OCATC.

[2] United States Computer Emergency Readiness Team. Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors [Press Release]. 16 Mar. 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

[3] McAfee Inc. “McAfree Labs Report Highlights Critical Challenges to Threat Intelligent Sharing” [Press Release]. Business Wire. 6 Apr. 2017. https://www.businesswire.com/news/home/20170405006423/en/McAfee-Labs-Report-Highlights-Critical-Challenges-Threat.

[4] Sterling, Bruce. “Mirai is Plenty Bad and Getting Worse.” Wired. 10 Dec. 2016. https://www.wired.com/beyond-the-beyond/2016/12/mirai-plenty-bad-getting-worse/.

[5] Barth, Bradley. “FYI, the OMG Mirai botnet variant turns IoT devices into proxy servers.” SC Magazine. 22 Feb. 2018. https://www.scmagazine.com/fyi-the-omg-mirai-botnet-variant-turns-iot-devices-into-proxy-servers/article/746128/.

[6] Franklin, Curtis Jr. “Mirai Variant Botnet Takes Aim at Financials.” Dark Reading. 4 Apr. 2018. https://www.darkreading.com/attacks-breaches/mirai-variant-botnet-takes-aim-at-financials/d/d-id/1331472?_mc=NL_DR_EDT_DR_daily_20180406&elq=5a047d1a53284b9daa7c44f75cc27d2f&elq_mid=84182&elq_cid=23418398&elqTrackId=47e1241517514b1da6dd514c0ca68fc6&cid=NL_DR_EDT_DR_daily_20180406&elqaid=84182&elqat=1&elqCampaignId=30345.

[7] Diversified Computer Resources. “Ransomware Cryptoworm--WannaCry.” Diversified Computer Resources. 23 Jun. 2017. https://dcrinc.net/2017/06/23/ransomware-cryptoworm-wannacry/.

[8] Graham, Chris. “NHS Cyber Attack: Everything you need to know about the ‘biggest ransomware’ offensive in history.” Telegraph. 20 May 2017. https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

[9] Ehrenfeld, Jesse M. “WannaCry, Cybersecurity and Health Information Technology: A Time to Act.” 24 May 2017. https://link.springer.com/article/10.1007%2Fs10916-017-0752-1.

[10] Chappell, Bill. “Petya Ransomware Hits At Least 65 Countries; Microsoft Traces it to Tax Software.” National Public Radio. 28 Jun. 2017. https://www.npr.org/sections/thetwo-way/2017/06/28/534679950/petya-ransomware-hits-at-least-65-countries-microsoft-traces-it-to-tax-software.

[11] Novet, Jonathan. “Maersk says June cyberattack could cost it up to $300 million.” CNBC. 16 Aug. 2017. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.

[12] Cabuhat, J. Casayuran, M. & Melgarejo, A. “Locky Ransomware Pushed Alongside FakeGlobe in Upgraded Spam Campaigns.” [Blog]. Trend Micro. 18 Sept. 2017. https://blog.trendmicro.com/trendlabs-security-intelligence/locky-ransomware-pushed-alongside-fakeglobe-upgraded-spam-campaigns/

ENDNOTES

13 Winton, Richard. "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating." Los Angeles Times. 18 Feb. 2016. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

14 Key Reinstallation Attacks. https://www.krackattacks.com/.

15 Tung, Liam. "Windows RDP flaw: 'Install Microsoft's patch, turn on your firewall.'" Zero Day. 14 Mar. 2018. https://www.zdnet.com/article/windows-rdp-flaw-install-microsofts-patch-turn-on-your-firewall/.

16 Truta, Filip. "How to protect yourself from the 'KRACK' Wi-Fi attack." Hot for Security. 21 Oct. 2017. https://hotforsecurity.bitdefender.com/blog/how-to-protect-yourself-from-the-krack-wi-fi-attack-19086.html.

17 Internet of Things (IoT) Cybersecurity Improvement Act of 2017. S.1691, 115th Cong. (2017).

18 Cyber Shield Act of 2017. S. 2020, 115th Cong. (2017).

19 Hunter, Pamela. "Margin of Error and Confidence Levels Made Simple." i Six Sigma. Accessed 22 Apr. 2018. https://www.isixsigma.com/tools-templates/sampling-data/margin-error-and-confidence-levels-made-simple/

IDENTIFY, ASSESS, AND RESPOND TO IoT THREATS

Pwnie Express closes the IoT security gap exposed by the deployment of IoT in the enterprise. By continuously identifying and assessing all devices and IoT systems, our IoT security platform prevents IoT based threats from disrupting business operations. All without the need for agents, or changes to network infrastructure. Our easy to deploy and operate SaaS platform, Pulse, makes it easy for security teams to identify, assess, and respond to IoT based threats to prevent business disruption:

- Identify—Discover, take inventory, and classify all IT and IoT devices and build a comprehensive identity for each device.
- Assess—Device behaviors are analyzed to understand system relationships and then monitored to detect threats and risks to business-critical systems.
- Respond—Ensure the safety and compliance of critical systems by preventing business disruption with directed response and shareable intelligence.

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