REPORT

Internet of Things
Cybersecurity Readiness

Trustwave®

Internet of Things Cybersecurity Readiness

Executive Summary

Trustwave commissioned industry analyst firm Osterman Research to conduct a survey of organizations in the context of their use of "Internet of Things" (IoT) technologies and challenges regarding introduction and security planning.

The survey was conducted primarily with mid-sized and large organizations in North America (median of 1,000 employees per organization). Individuals with applied security experience or knowledge were targeted. A total of 137 surveys were completed in November 2017.

Key takeaways from the survey include:

- Sixty-four percent of organizations are already using IoT technology to some extent, and 84 percent plan to do so by the end of 2018.

- Nearly three in five organizations can attribute some type of security incident to their use of IoT devices.

- Despite the significant current use of IoT devices and plans by most to increase their use, only 28 percent consider their IoT-related cyber security strategy to "very important."

- By giving such a low priority to security protections for their IoT devices and the networks to which they connect, decision makers are putting their organizations at serious risk of malware infections, denial-of-service attacks, data breaches and other threats.

- Decision makers' confidence in their ability to detect and protect against IoT-related security incidents is low, with only 38 percent "confident" or very confident."

- IT departments charged with vetting IoT devices rely too heavily on IoT vendors' security claims and too little on internal testing, third-party testing and published reviews of the devices they connect to their networks.

- Only 47 percent of the organizations surveyed consistently assess the IoT security risks they face from third-party partners' use of IoT technology.

- Only 49 percent of organizations have IoT patching policies in place and only about one-third patch their IoT devices within 24 hours after a fix becomes available.

Overview: Some Questions To Answer

How Is IoT Evolving Over Time?

We can safely say that we are in the relatively initial stages of the IoT market in terms of both the number of connected devices (relative to where we will be in five years) and their ability to connect. For example, Gartner estimated that there were 8.4 billion IoT devices in 2017, a figure that will grow to 20.4 billion devices by 2020[1]. While this is among the more recent forecasts, it is also dramatically more conservative than forecasts made just a few years prior. For example, a 2010 forecast by the CEO of Ericsson called for 50 billion devices by 2020. Even more optimistic was a 2012 forecast by IBM that there would be one trillion IoT devices by 2015[2].

While current forecasts for the growth of IoT are certainly more conservative than they were just a few years ago, IoT is clearly a rapidly growing market and one that needs to be top-of-mind for any IT or security professional moving forward. Today, IoT is primarily focused on connecting "things" to the internet in a way that is not markedly dissimilar to what we have seen occur over the past couple of decades. However, the evolution of IoT moving forward will be dominated by two primary considerations:

- Instead of simply connecting things to the internet – "IoT 1.0" – things will also be connected to other things, creating vastly more opportunities for functionality. As noted by Jim Chase of Texas Instruments, "the IoT creates an intelligent, invisible network fabric that can be sensed, controlled and programmed. IoT-enabled products employ embedded technology that allows them to communicate, directly or indirectly, with each other or the internet."[3]

- At the same time, the increased connectivity between things will create vastly more potential for security incidents to occur simply because of the dramatic increase in surface area available for bad actors to exploit. The problem will be exacerbated by the fact that the ability to create things and interconnect them – and the demand for this functionality – will outpace the security measures that organizations will take to protect against threats. Moreover, demand for newer, better, faster and cheaper IoT devices will drive some vendors to forgo building in the security necessary to prevent their devices from being exploited as a conduit for threats.

As discussed in this survey report, most organizations do not take IoT security as seriously as they should at a conceptual level, nor have they implemented the processes to ensure that the "things" they are connecting have been properly vetted.

1. http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/
2. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated
3. http://www.ti.com/lit/ml/swrb028/swrb028.pdf
4. http://www.techproresearch.com/downloads/internet-of-things-policy/
5. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
6. http://www.ioti.com/security/where-all-iot-malware-hiding
7. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
8. https://www.tripwire.com/state-of-security/security-data-protection/iot/stackoverflowin-story-iot-broke-internet/?NL=IOT-001UBER&Issue=IOT-001UBER_20170831_IOT-001UBER_651&sfvc4enews=42&cl=article_13_2
9. https://www.csoonline.com/article/3165419/security/hacker-stackoverflowin-pwning-printers-forcing-rogue-botnet-wa

What is an IoT Policy?

An IoT policy is not fundamentally different than a policy for any other device connected to a corporate network. A good example of an IoT policy is the one published by Tech Pro Research, some elements of which include[4]:

- "IoT devices may be business oriented (e.g., RFID tags to track inventory) consumer based (such as Fitbits), or a hybrid of both (like the Raspberry Pi, which offers an array of uses across the two sectors). The devices may be company-provided or employee-owned, such as through a BYOD policy.

- In general, IoT devices that are to be used for company operations should be purchased and installed by organizational personnel.

- It is allowable for employee-owned IoT devices to be used for business purposes, but they must be used in accordance with the organization's Bring-Your-Own-Device (BYOD) policy.

- The use of all IoT devices, whether company provided or employee owned, [is subject to the] IT department for approval. Only manager-level employees and above may request the usage and/or procurement of IoT devices.

- The IT department is responsible for identifying compatible platforms, purchasing equipment, and supporting organization-provided and authorized IoT devices."

In short, an IoT policy should describe what can be connected to the corporate network, how it can be used, who can own it, and who is in charge of approving it. Security must be a paramount consideration in the entire process of evaluating, selecting, deploying and managing IoT devices.

What are Some Key Dates in IoT History?

IoT represents an enormous security problem, dating back to 2008 with the development of the Hydra malware that specifically targeted IoT devices, namely routers. In addition:

- Perhaps the most infamous, and one of the earliest, IoT attacks was Stuxnet, designed specifically to target a "smart" industrial controller used in nuclear facilities. The malware was successful in destroying about one-quarter of the centrifuges it targeted, delaying a nuclear program by at least two years.[5]

- In 2015, IoT malware was successful in taking down a portion of an electrical grid, leaving 230,000 customers without power.[6]

- In October 2016, the Mirai botnet attacked Dyn servers, involving approximately 360,000 devices and taking down many high-traffic websites.[7]

- In early 2017, a teenage hacker was successful in discovering approximately 200,000 open printers that would allow printing over the internet – and he printed to them.[8] Approximately 150,000 printers were impacted and printed a message about the affected printer becoming part of a botnet[9].

Key Findings from the Survey

IoT Use is Growing Rapidly

Our research found that there is significant and growing use of IoT across a wide range of industries, as well as in organizations large and small. For example, as shown in Figure 1, nearly two-thirds of organizations have deployed some level of IoT technology, and another 20 percent plan to do so within the next 12 months. The result will be that by the end of 2018, only one in six organizations will not be using at least a minimal level of IoT technology for some business purpose.

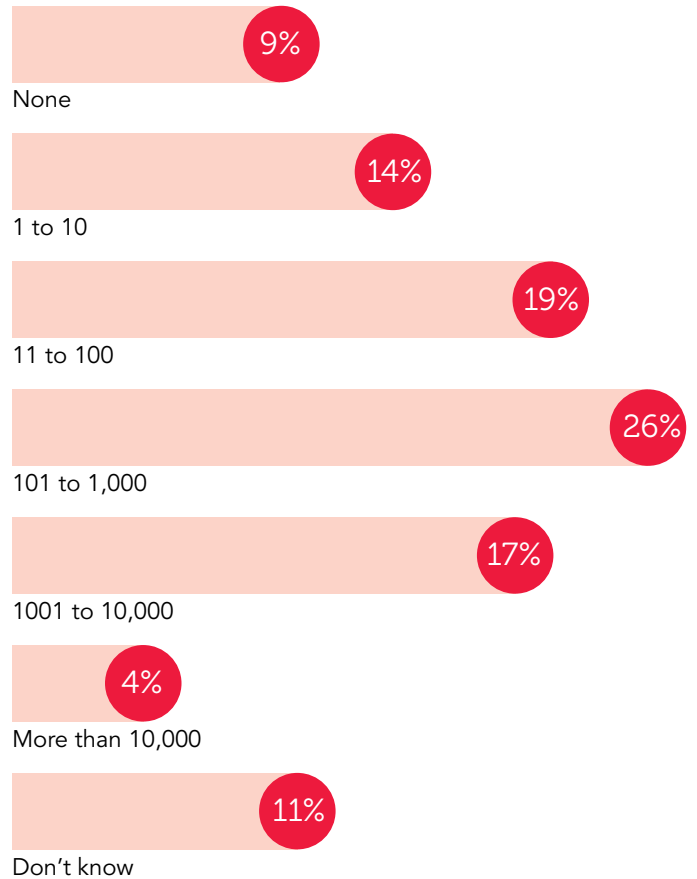| 64%	20%	17%
Yes	No, But we will be within the next year	No

Figure 1 Is Your Organization Currently Using IoT Technology?

Note: Figures do not total 100 percent due to rounding

As shown in Figure 2 there is significant discrepancy in the penetration of IoT devices in use, with some organizations having only a handful of these devices connected to the corporate network, while others have more than 10,000 such devices.
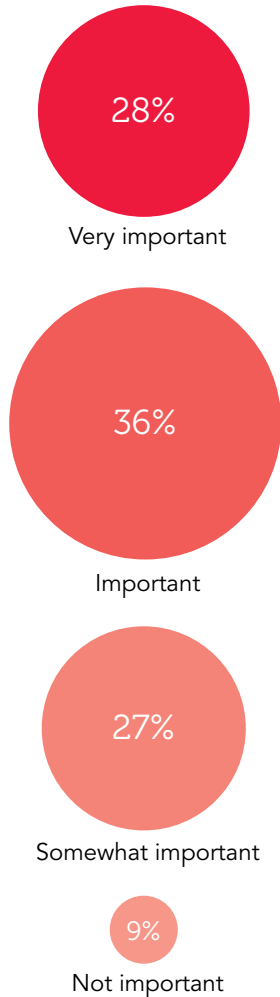
It is important to note that what appears to be a disconnect in the data between Figures 1 and 2 really isn't one. For example, while 64 percent of organizations are currently "using" IoT technology, Figure 2 indicates that 91 percent have IoT devices connected to the corporate network. Many organizations have IoT devices connected to the corporate network but, in a strict sense, are not "using" the technology because IT has not been involved in deploying them. For example, many perceive that personally owned devices like smartphones and tablets are IoT devices (and a case can be made that they are), yet these are not devices that corporate decision makers will consider are being "used" by the organization in the context of their IoT strategy.

None	9%
1 to 10	14%
11 to 100	19%
101 to 1,000	26%
1001 to 10,000	17%
More than 10,000	4%
Don't know	11%

Figure 2 How Many IoT Devices are Currently Connected to Your Corporate Network?

A Disparity Between IoT Use And Security

Even though more than 80 percent of organizations are currently or will be using IoT technology by the end of 2018, only 28 percent consider that their IoT security strategy is "very important" to the organization, as shown in Figure 3. More surprising, however, is that more than one-third of those surveyed believe that IoT security is only "somewhat" or "not" important.

Why the Disparity?

One of the reasons that so many organizations using IoT technology consider security to be relatively unimportant may be that IoT is not yet considered to be relevant. For example, as shown in Figure 4, only 57 percent of organizations plan to increase their penetration of IoT devices in the future, while 19 percent do not, and 23 percent are simply unsure of the future status of IoT. Given that many organizations have not yet established a business case for IoT, such as a solid return-on-investment analysis, it may be that security for IoT has been relegated to a much lower priority than it should be.

28%

Very important

36%

Important

27%

Somewhat important

9%

Not important

19%
No

23%
Not sure

57%
Yes
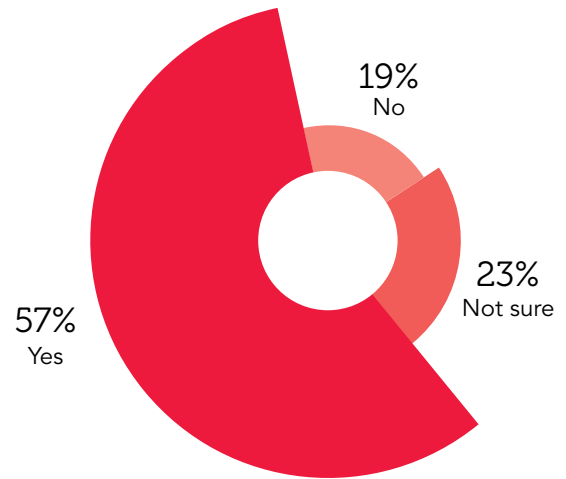
Figure 4 Does Your Organization Have Plans to Increase the Use of IoT in Your Operations?

Note: Figures do not total 100 percent due to rounding

Figure 3 Compared to the Other Cyber Security Priorities in Your Organization, How Critical is Your IoT Security Strategy?

Several Barriers Exist for IoT Adoption

Another issue that may be discouraging a more robust approach to IoT security is the fact that there are several important barriers to the adoption of IoT itself. For example, as shown in Figure 5, IoT use in many organizations is being inhibited by security concerns surrounding the technology – many decision makers may choose not to adopt IoT technology because of these concerns and, in turn, may place a lower emphasis on the overall security of IoT because of this barrier. Other reasons for not adopting IoT include its perceived lack of relevance to current operations, a lack of budget to adopt IoT technologies and lack of standardization.

57%

Security concerns

38%

Not relevant to operations

27%

Lack of budget

25%

Lack of standardization, such as for connectivity

23%

Integration challenges with existing business systems

22%

Size of IT and security team

21%

Market evolving to quickly

9%

Concerns over battery life

9%

Something else

Figure 5 Issues That Have Prevented Greater Adoption of IoT

Percentage Responding That an Issue Has Been a Factor

At first glance, comparing the data in Figure 3, where only 28 percent of decision makers believe that their IoT security strategy is "very important", seems to contradict the data in Figure 5, where 57 percent of respondents indicate that security concerns are a leading factor in preventing greater adoption of IoT. However, there are a couple of interpretations of these data points that are worth noting:
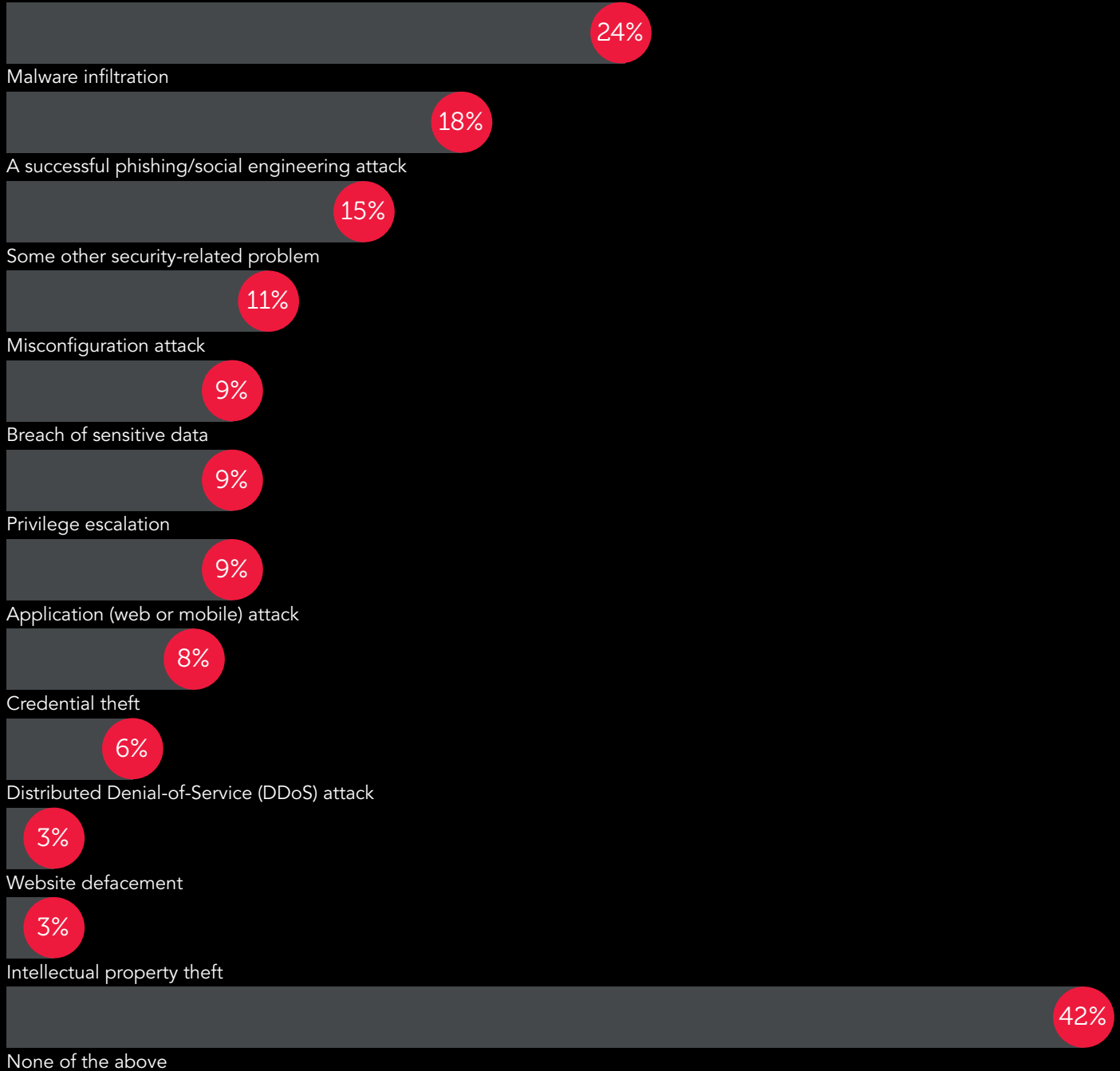
- The earlier figure shows the relative importance of IoT security strategy relative to other cyber security priorities, such as those focused on ransomware, phishing, business email compromise attacks, and the like. This doesn't mean that IoT security is not important, but it is not as important as security for these other problems – yet. Ransomware, for example, has resulted in the loss of billions of dollars, and the problem is growing exponentially. IoT security, while having the potential for becoming even worse than current security issues, simply has not yet become as top-of-mind as it will be.

- Some functional groups or departments within an organization may not be implementing IoT as much as they would like because their organization's IT or security functions have not yet given sufficient credibility or resources to protecting against IoT-based attacks. In other words, the comparatively low priority given to IoT security by an IT department may be the leading factor in preventing greater adoption of IoT noted in Figure 5. Further inhibiting the use of IoT is that many organizations lack internal security expertise and resources for IoT deployment and management.

A Lack of Focus on IoT Security is Unwise

Although decision makers may feel justified in not giving the security of IoT technology a high priority within their organizations, not having a robust and well-considered IoT security strategy is extremely unwise given the problems that organizations have already faced. As shown in Figure 6, most organizations have experienced at least one security incident, including actual attacks, attributable to IoT during the last 12 months. The most frequent problem encountered was malware infiltration via an IoT device, but phishing, social engineering and other problems were also common. Overall, 61 percent of the organizations surveyed that have deployed some level of IoT technology dealt with a security incident during the past year that they can trace back to an IoT device. However, we believe this understates the problem, since undoubtedly some organizations that have not yet deployed IoT have experienced some type of security problem related to it, perhaps introduced by an employee's or business partner's IoT device.

Spending on IoT security and giving it a high priority in the organization is essential as a means of reducing the risk associated with use of these devices. And it apparently pays off. One study found that IoT-enabled organizations that have not experienced a data breach spend up to 65 percent more on IoT security compared to IoT-enabled organizations that have experienced a breach.10
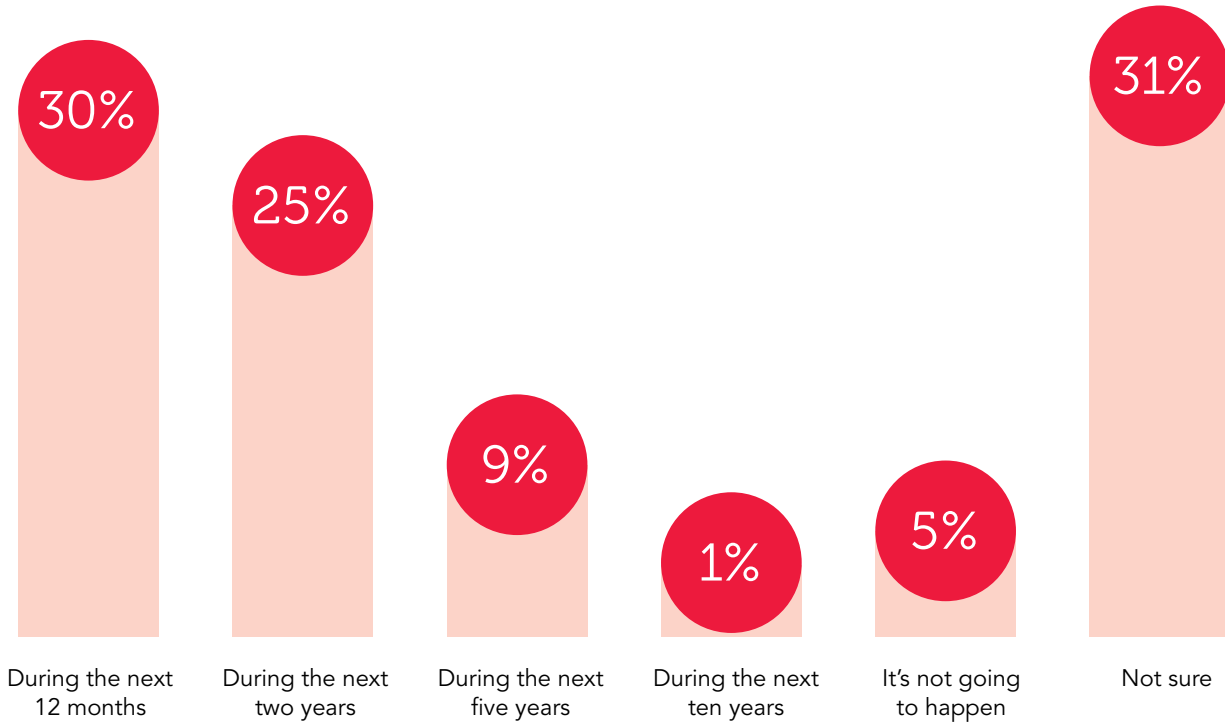
24%

Malware infiltration

18%

A successful phishing/social engineering attack

15%

Some other security-related problem

11%

Misconfiguration attack

9%

Breach of sensitive data

9%

Privilege escalation

9%

Application (web or mobile) attack

8%

Credential theft

6%

Distributed Denial-of-Service (DDoS) attack

3%

Website defacement

3%

Intellectual property theft

42%

None of the above

Figure 6 Security Incidents Attributable to IoT During the Previous 12 Months

10. https://internetofbusiness.com/half-us-iot-security-breach/

Most Believe They Will Experience an IoT Security Problem in the Future

The vast majority of those surveyed believe that their organizations will experience an IoT-related security problem at some point. As shown in Figure 7, 55 percent believe that it will happen during the next two years, and another 10 percent believe it will occur at some point beyond two years from now. While nearly one-third of those surveyed simply are not sure when an IoT-related security incident will happen, only five percent of those surveyed – just one in 20 – believe one will never happen.

30% During the next 12 months

25% During the next two years

9% During the next five years

1% During the next ten years

5% It's not going to happen

31% Not sure

Figure 7 Anticipated Timeframe for an IoT Security-Related Incident in the Future

Note: Figures do not total 100 percent due to rounding

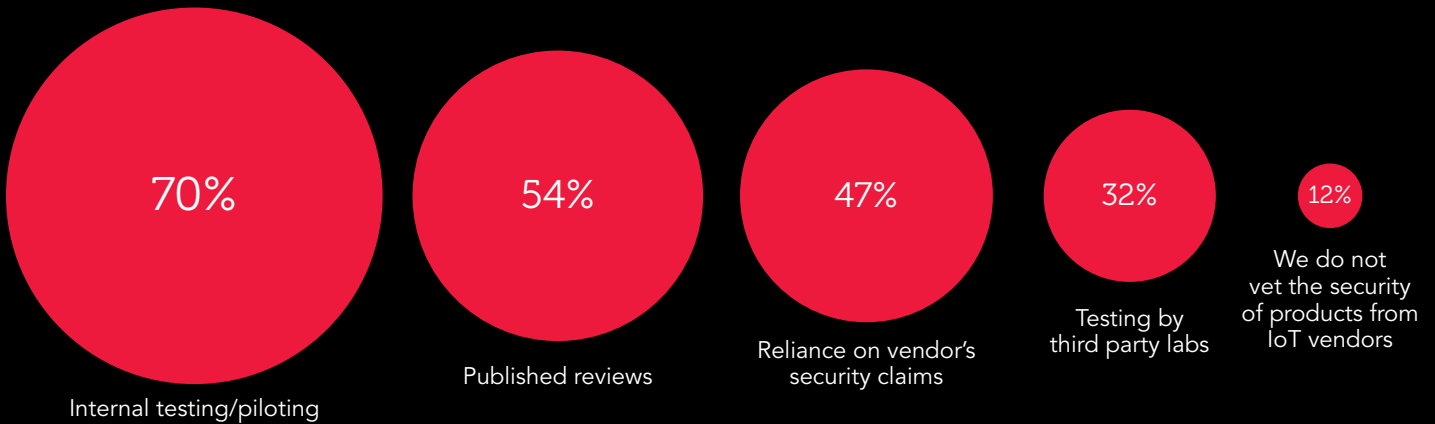## Confidence in IoT Security is Not High

The combination of a low emphasis placed on IoT security, the sizeable proportion of organizations in which security incidents have already occurred and the perception that future security incidents are a virtual certainty leaves decision makers with little confidence that they can defend against IoT-related security incidents. As shown in Figure 8, only 10 percent of those surveyed are "very" confident that they can detect and protect against IoT-related security incidents, while 62 percent are only "somewhat" or "not" confident that they can do so.

10% Very confident

28% Confident

49% Somewhat confident

13% Not confident

Figure 8 Confidence That Organizations Can Detect and Protect Against IoT-Related Security Incidents

## Problems in IoT Security Evaluation, Testing and Management

Although most organizations are proactively looking for security vulnerabilities in IoT devices, their current testing and evaluation practices are not adequate. As shown in Figure 9, only 70 percent of organizations conduct their own testing or piloting of these devices, only 54 percent use published reviews, and only 32 percent use third-party testing services. While IoT vendors' security claims are important in the vetting of network-connected devices, they should be considered carefully and only in conjunction with other testing processes and procedures.

70%
Internal testing/piloting

54%
Published reviews

47%
Reliance on vendor's security claims

32%
Testing by third party labs

12%
We do not vet the security of products from IoT vendors

Figure 9 Methods Used to Vet the Security of Products Purchased from IoT Vendors

Moreover, fewer than one-half of organizations consistently assess the IoT security risk posed by third-party partners, and another 34 percent do so only periodically, as shown in Figure 10. Nearly one in five organizations does not perform this risk assessment, leaving them vulnerable to security risks introduced by the use of third parties employing IoT devices.

not adequately vetted is the fact that one-half of organizations have no IoT patching policies in place, as shown in Figure 11. Moreover, as shown in Figure 12, nearly one-half of organizations report that it can take two or more days to fully implement an IoT patch after a fix is available.

19%
No

34%
Sometimes

47%
Yes

49% Yes / **No 51%**
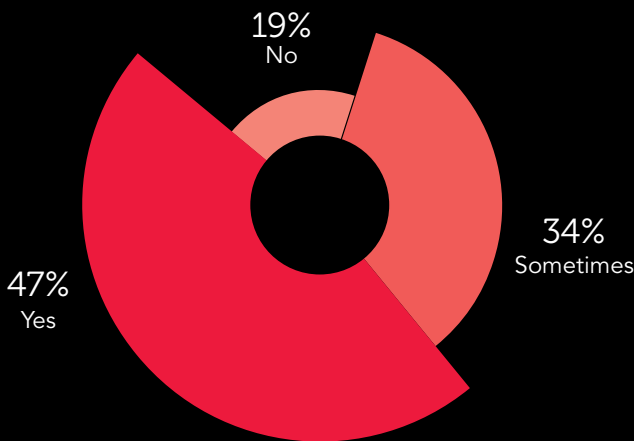
Figure 10 Do You Assess the IoT Security Risk Posed by Third-Party Partner?
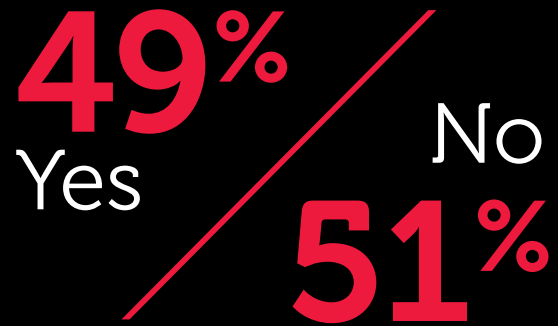
Figure 11 Does Your Organization Have IoT Patching Policies in Place?

| 7%	25%	20%	48%
Within an hour	Less than 24 hours	Up to 48 hours	48 or more hours
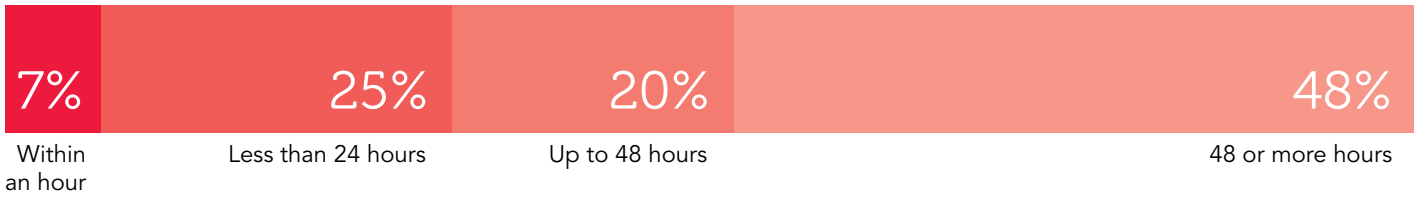
Figure 12 Length of Time Required to Fully Implement an IoT Patch Once It Has Been Issued

Obviously, an organization that does not have policies in place for patching IoT devices either will not patch these devices when updates become available, or they will do so on an inconsistent and haphazard basis. Further complicating the issue is that many IoT devices, particularly consumer-focused ones, are designed by a temporary team of contracted designers who is disbanded after the product has been developed. In cases like these, the vendor generally will not – and most often cannot – provide patches because no ongoing development team exists to create them.

Reliance on Vendors

Nearly one-half of organizations focus on external providers, such as security companies and independent consultants, to help them with their IoT security, as shown in Figure 13. However, most will look to their internal security teams, even though in many cases these teams are already overworked and may not represent the best option for many organizations that need both to learn and manage IoT security properly. Other sources of IoT security help include industry analyst firms, such as Gartner, Forrester, IDC and others.

76%
Internal team

46%
Security vendors

29%
Independent consultants

15%
Industry analyst firms
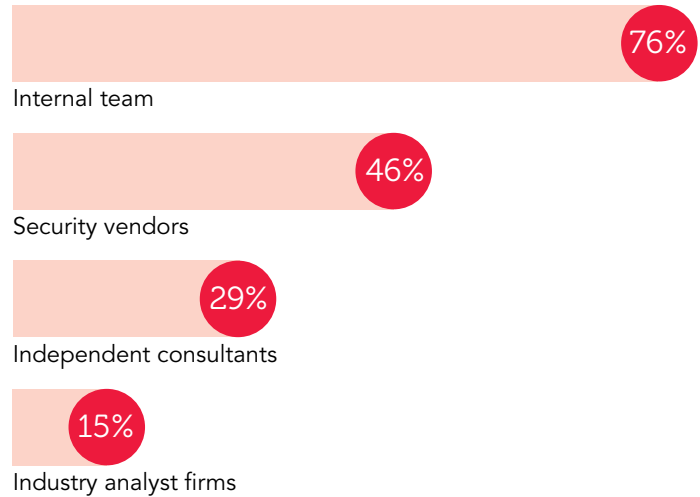
Figure 13 Extent to Which Various Sources Will be Used for Help with IoT Security Percentage Responding "Very Likely" or "Definitely Will" Consult

Conclusion

Most organizations that have deployed IoT devices are at serious risk of malware infection, denial-of-service attacks and other threats that could cause serious harm to their network infrastructure and the business itself. Moreover, vendors are offering IoT devices into a highly competitive market, pushing product to market as quickly as possible in many cases. The result is that security considerations often take a back seat to product features and timeliness, sometimes as a result of these competitive pressures and sometimes because many vendors lack the basic secure coding knowledge and vulnerability disclosure programs necessary to secure their products.

Decision makers generally place a low emphasis on IoT security, yet a substantial proportion of organizations are anticipating severe IoT security problems. For example, while only 10 percent are "very confident" that they can detect and protect against an IoT-related security incident, 95 percent believe that an IoT security incident will occur in the future.

Trustwave Recommendations

IoT is still in its infancy. We will continue to see a rise in IoT-based attacks, which can include sabotage, malware, denial-of-service and other malicious activity that could cause harm to your network infrastructure and the business itself.

The following are Trustwave's key recommendations to consider when assessing security risks and implementing IoT security plans.

IoT implementers should:

- Regularly scan and inventory your network to identify any non-traditional devices, which includes IoT.

- Research and vet IoT vendors before making new purchases. This includes studying their history and accessing security reports (which should be available on an ongoing basis).

- Trust and evaluate vendor claims, but also verify yourself through vendor risk management and security testing, which helps reveal vulnerabilities and weaknesses.

- Once you have identified or installed IoT devices, change the default passwords to unique, complex passwords to reduce risk of compromise.

- Implement an agile methodology for quickly patching IoT vulnerabilities to ensure that any attacks leveraging flawed devices are prevented or minimized.

- Perform continual and proactive threat hunting to search for advanced persistent threats that may have already crept into the network via vulnerable IoT devices.

- Restrict partner access to your network where practical to minimize the potential for IoT threats from entering.

- Engage with security vendors whenever possible, as most organizations lack the internal expertise or resources to manage their security in-house, particularly when trying to find weaknesses in the growing array of IoT devices.

IoT vendors (developers and manufacturers) should:

- Build security in from the start on the devices you manufacture, including web apps, mobile apps, servers and associated APIs that interact with IoT products.

- Monitor, confirm and advance the results of these efforts through ongoing security testing.

- Force users to change any default passwords before they use your products.

- Make the process easy for customers to both review your security processes during the vendor review period and stay protected once they adopt and deploy your products.

- Commit to ongoing security by delivering regular security updates to customers and making the process of applying the fixes as simple as possible.

- Managed security service companies can greatly augment internal security teams and help to make up not only for the limited resources that most in-house teams face, but also supplement the skills gap in some internal teams.

Methodology

Osterman Research conducted this survey in November 2017 with 137 members of its survey panel. To qualify for the survey, respondents had to be knowledgeable about and/or responsible for IoT-related security practices in their organizations. The mean number of employees at the organizations surveyed was just under 17,000. A wide range of industries were included in the survey. The survey was sponsored by and conducted on behalf of Trustwave. The survey has a margin of error of +/- 8.4 percent.

Trustwave®