A Forrester Consulting
Thought Leadership Paper
Commissioned By Cisco

March 2015

Security: The Vital Element Of The Internet Of Things

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

The *intelligent connectivity of physical devices* — known more popularly as the Internet of Things (IoT) —is rapidly increasing productivity and levels of communication and enabling numerous functions across organizations worldwide. Unfortunately, organizations' lack of understanding of IoT's specific security requirements hinders its growth potential. As such, an organization can only reap the promise of IoT's benefits if it thinks of the security element as a vital component of implementation.

In November 2014, Cisco commissioned Forrester Consulting to conduct a research study to understand the current and future security issues facing enterprise and government organizations in the IoT market. This study focused on addressing the following objectives: 1) discovering what types of IoT devices and applications enterprises are deploying now and in three to five years; 2) what types of technologies organizations are using to enable IoT solutions; 3) what types of security issues organizations face as they pursue IoT solutions; and 4) understanding how the risks associated with IoT will progress over the next five years.

The study methodology included an online survey of 336 respondents who were line-of-business, security, or IT/OT professionals with influence over decisions related to their firm's IoT strategy. Organizations in the US had 1,000-plus employees, and those in France, Germany, the UK, India, Japan, and China had 500-plus employees. These organizations represented a mix of vertical markets, including manufacturing, retail, healthcare, government, utilities, and transportation, as well as oil, gas, and petroleum. Additionally, seven 30-minute in-depth interviews were conducted with IT professionals in the same level of responsibility in the US.

KEY FINDINGS

Key findings from this study include:

- **IoT security is no longer an issue that organizations have to embrace sometime in the future — it is here and it is now.** Decision-makers recognize the value of IoT solutions to aid in numerous functions, ranging from infrastructure and energy management to healthcare systems and enhanced customer service. Indeed, a majority have either already deployed solutions or plan to do so within five years. Many of the IoT solutions enable organizations to innovate their processes and provide competitive differentiation.
- **Experiences with security breaches in IoT functions are giving decision-makers a moment of hesitation.** Organizations have experienced security breaches in the very functions in which they are deploying IoT solutions, prompting security to be a chief concern when rolling out their implementations. Over a third have experienced a security breach of any type, and concerns range from malicious hackers to threats to the safety of human life.
- **Organizations are not taking the necessary measures toward IoT security.** Most decision-makers recognize IoT security is inherently different than traditional IT security. However, some firms do not understand the high-level protocols and technologies required to secure IoT solutions, which prevents them from pursuing and fully implementing these IoT initiatives.
- **Many firms seek help from vendors that understand IoT-related security requirements.** A complete IoT security solution must address physical, networking, and data security components. Many organizations recognize that they need help with IoT security implementation and are seeking assistance from third-party vendors. Specifically, they seek vendors with expertise in providing IT infrastructure and security solutions that are reliable and scalable.

There Is Clear Momentum For Internet-Of-Things Adoption

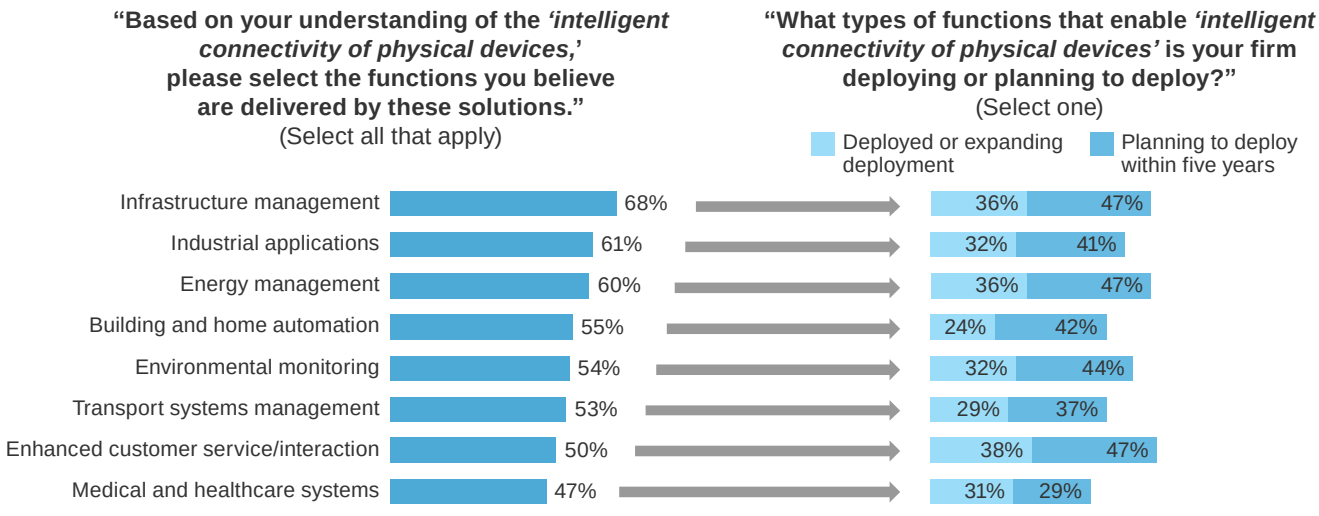
Organizations are increasingly embracing the *intelligent connectivity of physical devices* — often referred to as the Internet of Things — where critical business technology (BT) platforms are connected to physical assets. These IoT-enabled solutions cover a wide array of business and commercial applications and use cases driven by the ability to connect, monitor, and control tens of millions of Internet-connected devices, exchange information, and take autonomous action based on continuous input.[1]

IoT-enabled applications and solutions are evident across various industry and government sectors, including manufacturing, healthcare, transportation, oil/gas, utilities, energy, and water. Results from our survey of business, IT, and security professionals highlight current and future plans to deploy IoT functions:

› **There is clear momentum, with many firms deploying or planning to deploy IoT functions.** Organizations are deploying or planning to deploy a wide variety of IoT functions (see Figure 1). In fact, between 29% and 38% of firms have already deployed or are expanding deployment of IoT functions in transport systems, medical or healthcare systems, environmental monitoring, industrial applications, energy management, or infrastructure management. Expect continued deployment momentum for IoT solutions in the future, particularly in transportation systems, industrial applications, infrastructure management, environment monitoring, and energy management. Between 37% and 47% of surveyed firms are planning to deploy these IoT functions within five years.

› **Firms use IoT solutions to enhance efficiency, reduce costs, and enhance customer service.** As a director at a retail organization we interviewed stated, IoT solutions can help firms achieve many types of benefits to help them improve processes, enhance efficiencies, and reduce costs. Forty-five percent of respondents said IoT solutions can help them manage, monitor, and efficiently use energy or power resources. In addition, 43% of respondents stated that IoT solutions can help reduce operational expenses or costs. Other benefits identified by 38% to 40% of firms include improving safety, managing risk, and improving customer experiences.

FIGURE 1
Implementation Timelines Highlight Many Current And Planned Internet-Of-Things-Enabled Initiatives



Base: 336 Internet-of-Things decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

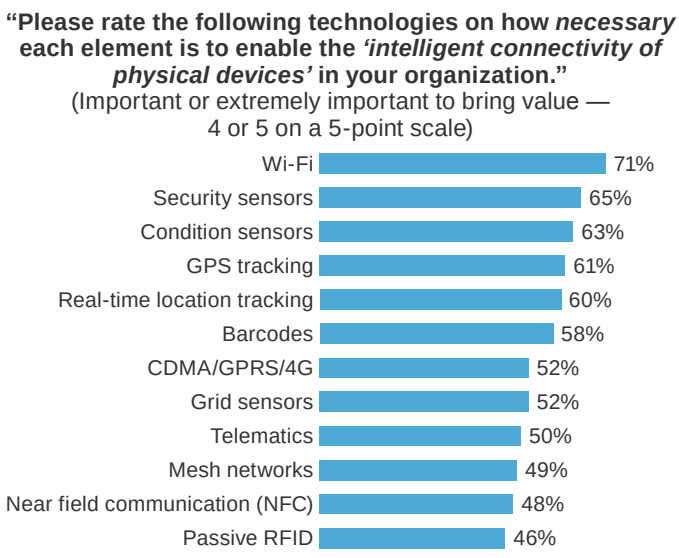
"We see benefits in fraud detection, general safety, marketing improvements, analytic and tracking, price planning, revenue generation, and returns management."

— Director at a retail organization

› **Many different technology elements are necessary to enable IoT solutions.** Decision-makers identified various types of technologies as necessary to enable IoT solutions (see Figure 2). Leading the way is a Wi-Fi infrastructure, which was identified as a necessary element by 71% of firms. Sensors and location tracking functions are also necessary to capture the location, condition, and status of products and assets. Between 60% and 65% of surveyed firms stated that real-time location tracking, GPS tracking, condition sensors, or security sensors are necessary elements of IoT solutions. These security sensors can be used to enable IoT applications, including surveillance solutions to monitor buildings, office sites, or even workers.

FIGURE 2

A Wide Selection Of Technologies Is Necessary To Enable IoT Solutions



Base: 336 Internet-of-Things decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

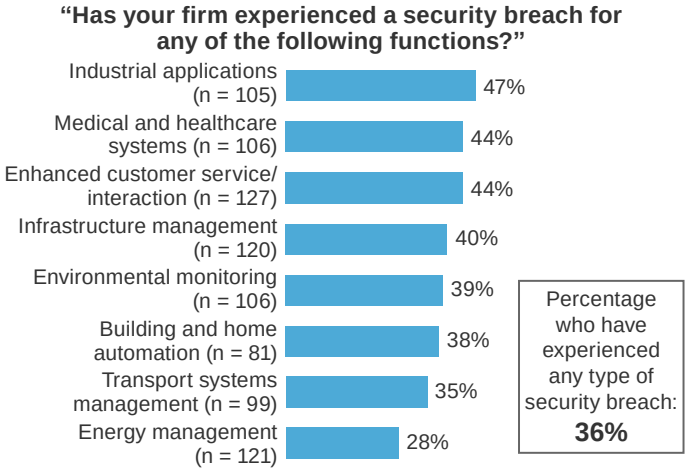
Security Is Of Paramount Concern When Implementing Internet-Of-Things Solutions

As adoption grows, business, IT, and security professionals tasked with deploying IoT applications and solutions must address significant paradigm changes as well as operational, strategic, and business challenges. As they face various internal and external security issues such as network attacks, malware, malicious software, and external hackers (see Figure 3), decision-makers must understand:

› **IoT security is not a future issue that organizations have yet to embrace — it is here and it is now**. Twenty-eight percent to 47% of organizations have experienced breaches for each function where they are planning to deploy or have already deployed IoT solutions. IoT is a tidal wave of technology that is network-connected and has already permeated industries from manufacturing to healthcare. Breach quantity in IoT, while still lower than traditional computing breach quantity, is at a level where awareness of IoT-specific security issues must be mandatory.

FIGURE 3

Organizations Are Experiencing Security Breaches In Functions Where They Seek To Enable Internet-Of-Things Solutions



Base: Internet-of-Things decision-makers who are deploying functions

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

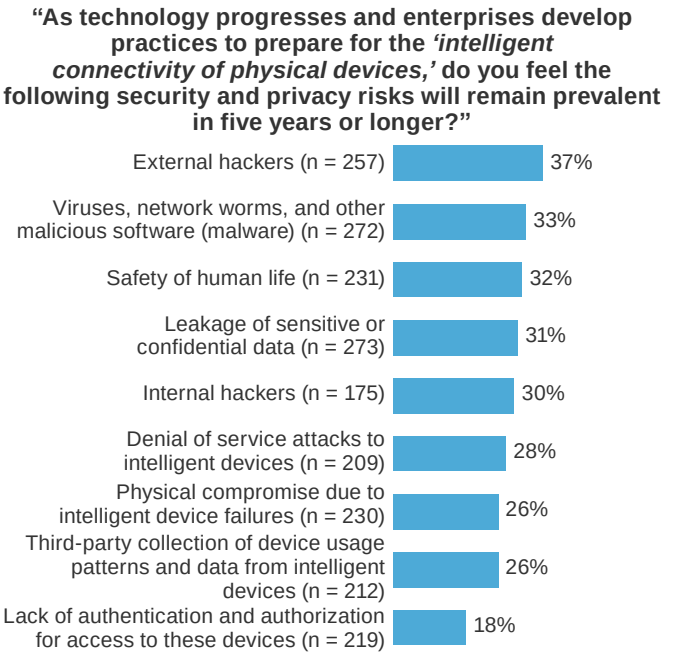
FORRESTER®

› **Security concerns are growing in tandem with IoT adoption.** The swift and steady adoption of IoT solutions raises concerns among decision-makers on IoT's security implications. A manager at a government organization stated, "The more we add to [IoT], the more we are concerned with security." These concerns plant the seeds of doubt as decision-makers envision the implications of these malicious attacks — for example, the manager at a government organization specifically cited fears of a hacker taking over road displays.

Furthermore, these fears are not going away anytime soon. Decision-makers feel that a wide array of security and privacy risks will continue to threaten the IoT space (see Figure 4):

› **Decision-makers feel malicious threats will remain prevalent over the next five years.** It is apparent to many decision-makers that the next five years will see an increase in malicious threats to the IoT space. Many feel that threats from external hackers (37%), malware (33%), internal hackers (30%), and denial of service attacks (28%) will not be mitigated in five years' time and will remain pervasive. In many ways, the IoT state of security is similar to the state of security for web applications in the late 1990s — a very large, unexplored, threat landscape exists that is ripe for exploitation. Decision-makers feel that security in the IoT space requires innovation that may take years to properly deliver.

FIGURE 4
Decision-Makers Believe Numerous Security And Privacy Risks Will Remain Prevalent Five Years From Now



Base: Internet-of- Things decision-makers who rated the security/privacy risks as important

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

› **Privacy remains relevant in the Internet of Things.** IoT extends the computing consciousness into the realm of physical goods and sensors as never before. These sensors provide context to the decisions and business objectives being automated by the IoT systems themselves. Thirty-one percent of decision-makers feel that privacy concerns will remain an important factor in the security of IoT over the next five years. As the level of context and data collected by IoT systems increases, the risk for privacy violations similarly increases.

› **As such, the challenge and importance of effective security solutions are imperative in the successful implementation of IoT solutions.** Decision-makers must evaluate and integrate a wide variety of technology elements to achieve a seamless IoT deployment, but addressing the security element is key. Security ranks highest, both in terms of importance (76%) and in the level of challenge (58%) it presents, above all technology elements (see Figure 5). A lack of strong security controls on the IoT solutions supporting enterprise systems will result in the erosion of confidence in the IT and security teams.

Organizations Don't Know How To Approach Internet-Of-Things-Specific Security

The concern for risk is compounded by the unfortunate fact that most decision-makers in our study are unaware of how to properly secure IoT solutions. As security approaches are playing catch-up to IoT adoption, they lack a comprehensive strategy and the necessary IoT-specific technical expertise:

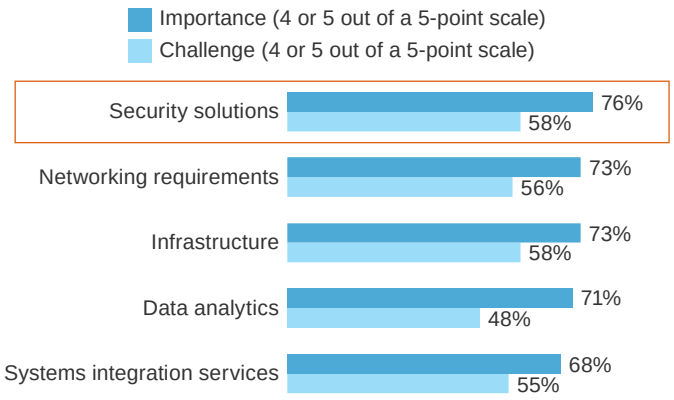
› **Despite acknowledging that IoT implementation is increasing, there is no consensus on the safest, most efficient way forward.** Organizations do not wish to extend their IT infrastructure without a direct mapping to the improved customer interactions and revenue. Increasing the threat landscape requires security investment to offset the added risk. Organizations have difficulty understanding the technical risk of IoT and

FIGURE 5

Both The Importance And Challenge Of Seeking Security Solutions Are Top Of Mind When Implementing Internet-Of-Things Solutions

"Please rate the following elements based on how *important* and how much of a *challenge* each element is to implementing applications and solutions that use the *'intelligent connectivity of physical devices'* in your organization."

(Rate on a 1-to-5 point scale, showing top 5 in importance)



Base: 336 Internet-of-Things decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

business improvement impact, making the decision to limit IoT implementation an understandable choice. To put it bluntly, a director at a manufacturing organization summarizes this fact when saying that the organization is "not on the bleeding edge," and its primary drive for its IoT initiatives is to "implement something that really reduces costs and gets [it] closer to [its] customers."

This mindset puts a bottleneck on IoT adoption. Although adoption has momentum, the weight of security concerns drags down adoption speeds, causing organizations to fall short of their full potential. Additionally:

› **Most organizations have a minimal level of knowledge of IoT security processes and procedures.** As they implement IoT technologies, organizations look to device vendors to provide security and patches, with some stating that security is a high enough priority to limit or stop implementation. As a director at a government organization stated, "The convenience factor doesn't outweigh the risk." Without a deeper understanding of the security processes and procedures necessary for IoT, organizations must attempt to balance between the promised functionality of the IoT device and a mode of security they are familiar with. As a result, IoT adoption rates, while gaining momentum, are not growing as fast as they could if security concerns were mitigated.

› **Organizations are lacking the technical skills required to assess the security of IoT devices used internally or as innovative outbound product enhancements, making it difficult to effectively scale IoT deployments.** Before an organization can support additional IoT systems, it has to understand how to deploy and secure the new systems. Decision-makers acknowledge as much, with a director of a manufacturing organization stating that "devices have to be hardened and tested. They have to have people who know how to test the functionality *and* the security."

> *"We expect that IoT will be targeted [by hackers]. Devices have to be hardened and tested. They have to have people who know how to test the functionality* and *the security."*
>
> — Director at a manufacturing organization

› **As most organizations are generally unsure about how to apply proper security to IoT, their approaches are cautious, lacking, or nonexistent.** The traditional model of security is different when applied to IoT devices such as basic sensors and data collectors. To be able to withstand the large number of devices expected with IoT, a new approach to security will be created. Unfortunately, organizations don't yet understand what this new approach should look like. For example, a manager in a government organization stated: "Security is different in IoT because of the challenges, risk management, and business impact analysis. But I don't know at this point if I understand the differences today to even explain it effectively." As a result, decision-makers in our study often default to applying what has worked for them in the past — standard IT fixes and solutions that do not address the unique complexities of IoT.

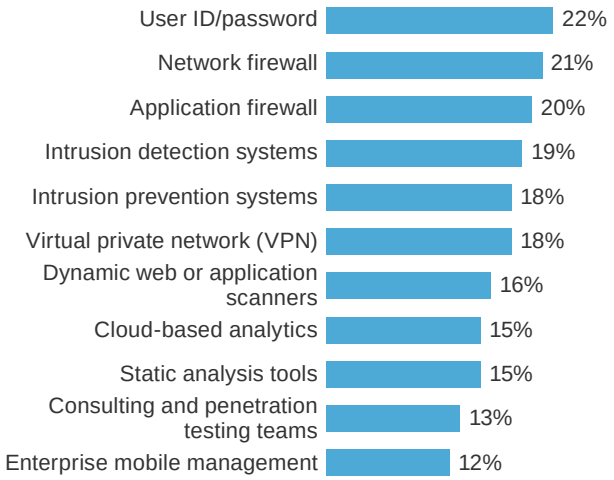
› **Understanding new communication protocols, hardware types, and obscure operating systems is difficult, making IoT security an incredible challenge.** Organizations are quickly overwhelmed with the changes required in risk management, technical security

understanding, and business impact. In some extreme cases, this results in a "fail open" scenario where organizations accept that they have the unquantified risk, but with no way to understand it, so they default to the fundamental security controls that they have used in the past. Indeed, a manager at a government organization told us that her agency has "no more additional security technologies [to secure IoT] other than the typical login password." Indeed, user IDs and passwords are believed by decision-makers to be able to perfectly secure IoT solutions, with no need for more robust security technologies (see Figure 6).

FIGURE6

Decision-Makers Believe Some Of The Most Basic Measures Are Able To Perfectly Secure IoT Solutions

"Please rate the following security technologies in their ability to apply security controls to *'intelligent connectivity of physical devices.'"*
(Can perfectly secure intelligent connected physical devices — 5 on a 5-point scale)



Base: 336 Internet-of-Things decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

Vendor Assistance Is Critical In Establishing Sufficient Security Protocols For Internet-Of-Things Implementations

The dearth of sufficient security understanding around this space is a clear signal that organizations need to seek help from vendors that possess technical know-how of how IoT functions, as well as an understanding of IoT's specific security requirements. To this point, our study has found that:

› **Many organizations are currently seeking assistance from IT infrastructure or security solution providers to fill gaps.** In addressing the challenges associated with deploying IoT functions, organizations often seek assistance from third-party partners. In particular, 50% of surveyed firms would seek assistance from IT infrastructure providers, and 47% would seek assistance from security solution providers. Key characteristics of these third-party vendors include security expertise; reliable, scalable solutions; and customer support capabilities. These decision-makers recognize the importance of addressing security, reliability, and scalability issues but need third-party assistance in these areas as they expand the breadth and depth of IoT solutions throughout their operations. A director at a healthcare organization articulates this by saying: "I would have to question the vendors and require security to be built in from day one. I don't know what's out there from a security perspective. It's a concern, but I have no idea how to solve it."

"I would have to question the vendors and require security to be built in from day one. I don't know what's out there from a security perspective. It's a concern, but I have no idea how to solve it."

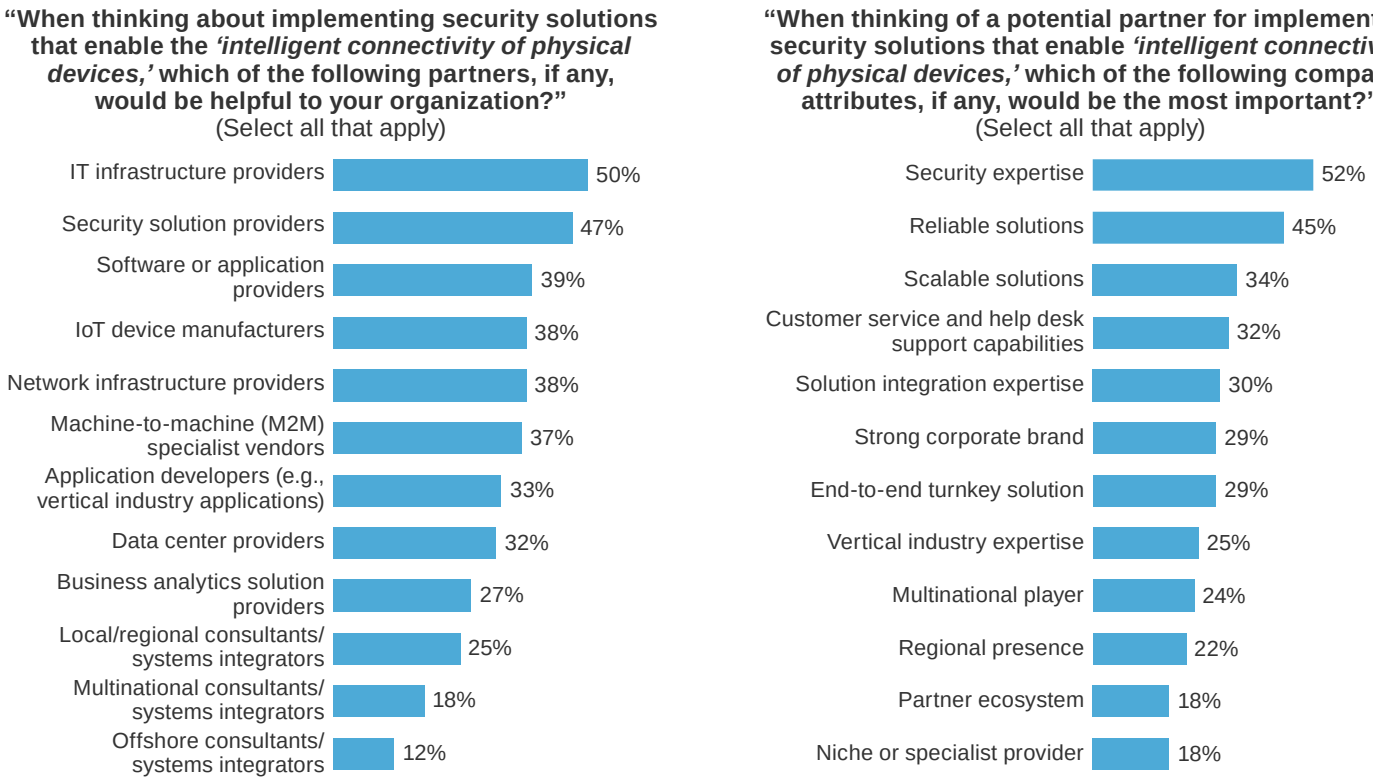
— Director at a healthcare organization

› **Organizations turn to IT infrastructure and security solution providers for deployment assistance.** IoT is currently seen as an extension of the infrastructure of an organization. Decision-makers are looking at the infrastructure and security solution providers to help them understand the risk tradeoffs of the IoT landscape (see Figure 7). Deployment and security groups must quickly educate themselves on what IoT devices their organization currently has or is planning for. If your executive team isn't asking you about IoT security today, they will be soon.

› **Important characteristics of partners include reliable and scalable solutions, as well as security expertise.** Advanced organizations that may be pushing the bleeding edge of IoT implementation are expecting to leverage partner expertise around security and scalability of IoT deployment (see Figure 7). Once the organization realizes the return on the investment, the risk-reward ratio will shift, resulting in a quickening implementation pace. Vendors, service providers, and internal IT groups must get ahead of this curve by improving their expertise in these areas, so they can support the emerging computing models of the future.

FIGURE 7

Decision-Makers Acknowledge The Value Of Vendors Known For Security Expertise Reliability And The Ability To Scale



Base: 336 Internet-of-Things decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

Key Recommendations

The promise of the Internet of Things can only be fully realized when fears about the very real security implications are assuaged. As such, organizations would do well to take advantage of the available expertise in the marketplace and learn from the experts before attempting to tackle the issues themselves. To this point:

- **Recognize that Internet-of-Things solutions are a reality for many firms today.** Results from our study of organizations across many different industry and government sectors highlight the fact that many different types of IoT functions and applications are being deployed. These IoT solutions enable organizations to transform processes, enhance operations, and improve efficiencies in many different sectors. As a result, decision-makers must evaluate key areas of IoT solution momentum, including infrastructure management, energy management, industrial applications, and environmental monitoring to pinpoint where IoT deployment makes the most sense. Business, IT, and security decision-makers must then work together to identify, evaluate, and prioritize the relevant IoT functions and applications for their organization. This evaluation process must account for the unique regulatory requirements, security risks, and competitive landscape facing each firm.
- **Prioritize opportunities and risks of deploying Internet-of-Things solutions within your firm.** When identifying, evaluating, and prioritizing the IoT functions in their organization, decision-makers must also keep a vigilant eye on the potential risks of that deployment. They must develop a comprehensive understanding of their level of exposure to risk to IoT-associated threats by conducting a full audit of their security capabilities. Only then can organizations make a smart and concerted leap toward full IoT adoption.
- **Prioritize security as a key Internet-of-Things technology element that is critical for deployment success.** Both the threats and promises of IoT are very real, requiring organizations to invest in both security technology and IoT-specific technical know-how. Simple password protection is not sufficient — security decision-makers must think more along the lines of using contextual-aware security that incorporates multiple factors into the authentication decision. This could manifest as a bidirectional digital certificate, plus security passphrase or SSH key. It is important to understand that simply applying traditional IT solutions and practices to IoT initiatives is a common occurrence but a poor approach. Deploying and securing IoT solutions can be complex, and therefore requires a specific skill set.
- **Evaluate third-party partners with expertise to enable a seamless solution implementation.** Deploying an end-to-end IoT solution requires an array of technology, network, device, and security elements. IoT stakeholders must identify and evaluate opportunities to partner with third-party vendors, including IT infrastructure and security solution providers that can assist them with IoT solution deployment — particularly if their security technical knowledge does not match what is necessary to secure IoT. Key characteristics to consider when evaluating these third-party vendors include security expertise, as well as the scalability and reliability of their solutions.

Appendix A: Methodology

This study surveyed 336 respondents who were line-of-business, security, or IT/OT professionals with influence over decisions related to their firm's IoT strategy. Organizations in the US had 1,000-plus employees, and those in France, Germany, the UK, India, Japan, and China had 500-plus employees. These organizations represented a mix of vertical markets, including manufacturing, retail, healthcare, government, utilities, and transportation, as well as oil, gas, and petroleum. Additionally, seven 30-minute in-depth interviews were conducted with IT professionals in the same level of responsibility in the US. The study began in June 2014 and was completed in November 2014.

Appendix B: Endnotes

[1] Source: "Mapping The Connected World," Forrester Research, Inc., October 31, 2013.