Security concerns escalate as IoT expands

Market insights on the state of IoT security.

RESEARCH STUDY

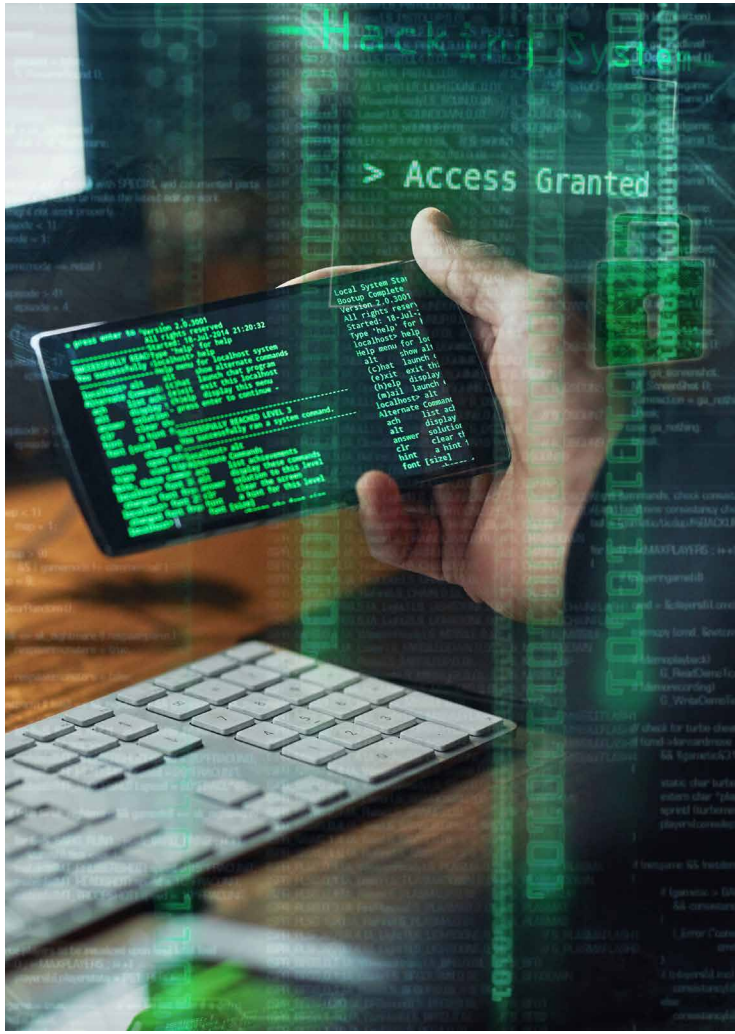
STRENGTHENING SECURITY

Mitigating IoT security risks in an era of rising threats

One major trend poised to have a transformative impact on the digital economy of the future is the Internet of Things (IoT). The IoT is already bringing advanced capabilities to real-world applications, from connected cars and homes to smart utility meters and health monitoring. According to one estimate, the number of connected devices worldwide is expected to jump 12 percent on average annually, from nearly 27 billion in 2017 to 125 billion in 2030.[1]

The operation of the IoT is based on several core underlying technologies. At the center of these are communications networks, hardware devices and components such as sensors, wireless instruments and software. Like any IT system, networks and devices are susceptible to manipulation, disruption and intrusion. And because these devices are connected to one another, if one device is compromised, a hacker has the opportunity to connect to multiple other devices on the network.

While the IoT offers vast benefits, it also offers an attractive entry point for bad actors to gain access to systems that were assumed to be secure. At a time when security environments are already experiencing scalability and cost pressures, IoT security experts face the monumental task of finding a way to protect networks and devices from an ever-growing array of potential threats that could compromise personal privacy and threaten public safety.



42%

of companies have experienced a direct breach in the past two years.

59%

find compliance with security regulations difficult.

Executive summary: Understanding the risks and challenges of IoT

To better understand how companies are preparing for and responding to current and emerging IoT security threats, UL teamed with Bloomberg Next to conduct a survey of executives and senior managers across key industry sectors, including retail, manufacturing and healthcare. The survey targeted decision makers responsible for coordination, oversight and management of IoT security practices and initiatives within their respective organizations.

The study focused on addressing several core objectives:

1. Assess the global scope and depth of IoT enablement across processes, products, and services.
2. Understand attitudes regarding IoT vulnerability, areas of concern and how risk is assessed and mitigated.
3. Determine familiarity with security regulations and assess variations in compliance difficulty among industries and geographic regions.

The findings reveal fresh insights into the way organizations view IoT security risks and the steps they are taking to address vulnerabilities, protect critical assets, and meet new and emerging regulatory requirements. The threat of a network intrusion is a persistent concern among IoT managers—and it should be.

As security concerns grow in parallel with IoT adoption, the findings underscore the difficulties companies face in their effort to combat rising threats. In other key areas, the survey found that:

- IoT security is a pervasive concern across industry sectors, with 49 percent of companies indicating they were "very concerned" about cybersecurity in general.
- Though security readiness lags, global IoT expansion continues. Asia has the biggest growing need for security risk mitigation, given the rapid increase of IoT deployments in the region.
- Companies that have experienced a security breach are actively taking or have completed more steps to mitigate risks compared to those that have not experienced a breach.
- Breaches lead companies to change their approach. More specifically, tapping outside resources is more common among those who have experienced a breach.
- The majority of organizations (59 percent) find compliance with security regulations difficult. This difficulty was notably higher in Europe (71 percent), which coincides with a lower level of familiarity with compliance standards.
- When it comes to implementing a new IoT security plan, 52 percent of companies plan to work with a third-party expert.

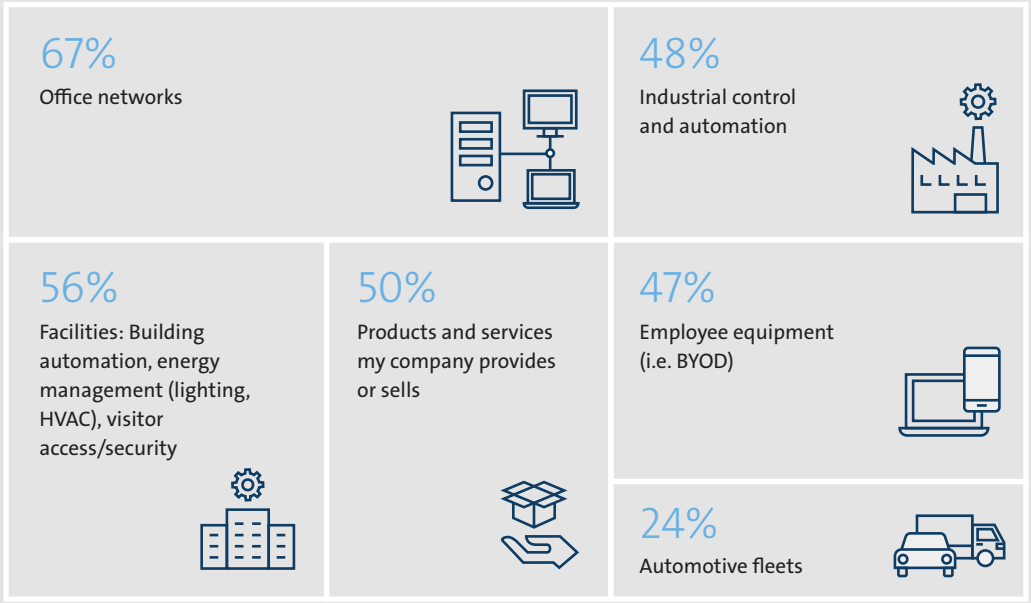
Nearly half

of the companies surveyed reported they have experienced a direct security breach in the past two years. For U.S. companies, this figure was notably higher at 53 percent.

IoT deployments continue to grow

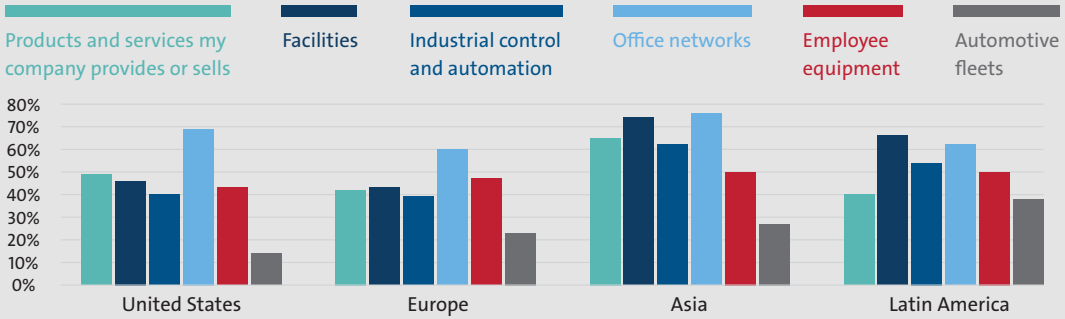
Rapid advancements in manufacturing, electronics and IT sectors are intensifying the demand for IoT products and services. Our survey shows that companies are implementing IoT functions across a range of ecosystems. Office networks were the most common deployment setting (67 percent), followed by facilities/buildings (56 percent), products and services (50 percent), industrial automation and automation controls (48 percent) and employee devices and equipment (47 percent).

Top environments where companies use IoT



Companies in Asia leverage a wider range of IoT-enabled settings.

% of companies where each setting is IoT enabled

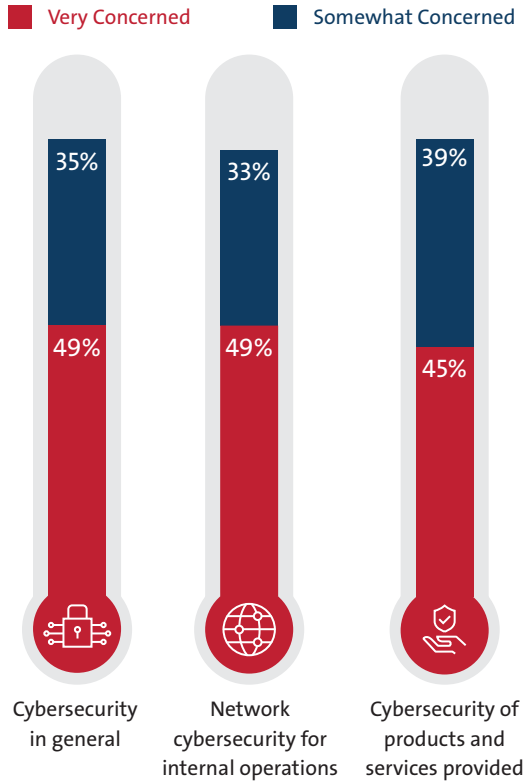


The United States is the largest market for IoT deployments, followed by Europe and Asia. Asia has the biggest growing need for cybersecurity risk mitigation given the rapid increase and wider range of IoT-enabled functions. Latin America is also experiencing substantial growth, particularly in the smart city market where IoT applications are being deployed across utility, public transport and healthcare settings. This region will be important to monitor as the market matures.

Growing concerns parallel IoT adoption

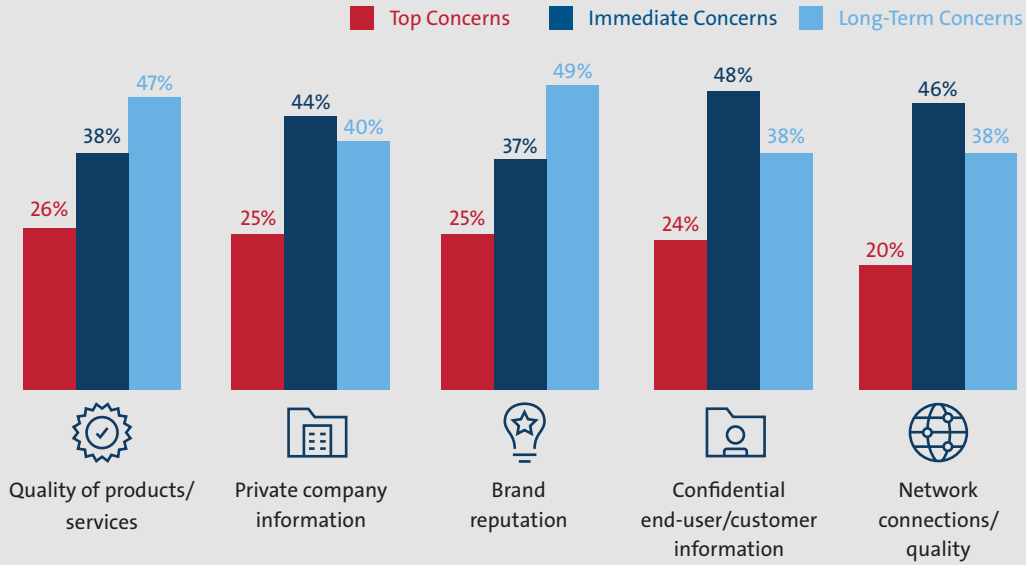
The risk of a security breach is a pervasive concern among company managers and executives, with nearly half of companies indicating they were “very concerned” about cybersecurity in general.

Security threats create heightened levels of concern among company executives.



The desire to support and protect brand value is evident as customer experience issues drive most security concerns. More specifically, product quality, end-user trust and brand reputation are among the top concerns and tend to be long-term issues. Concerns around the privacy of end-user information and the network itself are more immediate.

Customer experience issues drive most long-term security concerns.



Areas of concern vary within specific industries:

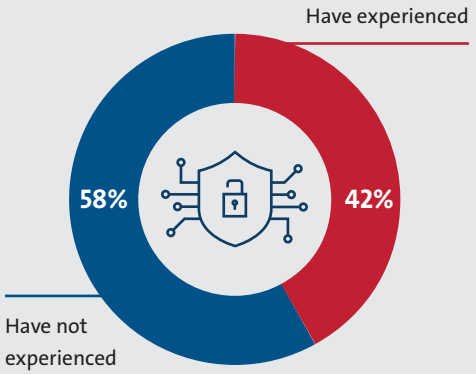
- In the healthcare sector, protecting confidential end-user information takes priority.
- In manufacturing, network connection and quality rise to the top.
- In retail, brand reputation and customer trust are more important.

The hidden peril of undetected intrusions

Each new IoT device adds another attack pathway into IT systems and it only requires one vulnerability in a single device to threaten an entire ecosystem. Our survey showed that 42 percent of companies have experienced a direct breach in the past two years—motivating them to strengthen their defenses.

While the number of reported breaches is alarming, perhaps more disturbing is the pervasive inability among many companies to detect an ongoing data breach—creating a widespread lack of awareness. In fact, nearly half (48 percent) of businesses aren't able to detect breaches when they occur, according to a research report released by digital security company Gemalto.[2]

Almost half of companies have experienced a direct breach.



200 days
— the average length of time it takes to detect an intrusion.[3]

One major challenge is the extended length of time it often takes to uncover a breach, which can elevate a company's risk profile and create false assumptions around the potential impact and scope of threat danger. According to a report from Verizon, dwell time (how long it takes to detect an intrusion) is averaging more than 200 days—despite it taking just minutes to compromise sensitive data.[3]

While these findings have compelling implications, the more immediate question is: Of the 55 percent of companies in our study that have not experienced a breach, how many of them have already suffered an intrusion but don't yet know it?

Network activity logs are one the most critical sources of threat detection, but research shows that only 21 percent of organizations are using their log data effectively.[4] Rarely are these logs proactively checked for the possibility of an unauthorized access or security incident. As a result, most organizations are oblivious of the hacks and attacks that are occurring within their IoT systems.

Nearly half
of businesses aren't able to detect breaches when they occur.[2]

Preparing for an attack: From complacency to readiness

The risks with connected devices are broadly dynamic since the IoT itself is adapting and expanding at such a rapid pace. There also are fewer barriers for attackers to hurdle when trying to breach an IoT device. Unlike a laptop or desktop computer, which is typically equipped with security software and enjoys the benefit of regular security updates, an IoT device's only defense may be a default username and password.

The IoT also generates data with a wide range of security requirements. Some data streams require minimal protection while others may include highly sensitive information—such as financial data and those that contain confidential medical records—and require more robust security measures. The rapid growth and maturity of IoT environments bring with it corresponding interest in attacking business assets for financial advantage or to simply cause chaos and disruption. While companies worldwide are concerned about IoT breaches, preparation measures lag behind—even as the IoT expands.

Companies often underestimate the possibility of a disaster and are grossly underprepared for breaches WHEN they happen.

Companies that have experienced a breach are actively taking or have completed more steps to resolve cybersecurity concerns, and thus are better prepared.

Hiring outside experts to help manage IoT security processes is more common among those who have experienced a breach.

IoT attacks—From potential to reality

Industries that support critical infrastructure are especially vulnerable to IoT security breaches that can compromise sensitive data and disrupt mission-critical operations. In the past several years alone, there have been a number of high-profile examples of how software vulnerabilities can lead to potentially costly and dangerous consequences.

In 2016, a breach perpetrated by the Mirai botnet infected a number of IoT devices and then used them to initiate a large DDoS (Distributed Denial of Service) attack on domain service provider Dyn.[5] The attack took down a long list of websites, including Shopify, Netflix and Twitter. The incident set a dangerous precedent for how connected devices could be "recruited" by attackers and used for malicious purposes without the device owners ever knowing about it.

At the 2016 DEF CON security conference, door locks, thermostats, refrigerators and wheelchairs were among the IoT devices that fell to hackers during a series of demonstrations.[6] The types of vulnerabilities identified during the event ranged from poor design decisions to coding flaws. In all, 47 vulnerabilities affecting 23 IoT-enabled items from 21 manufacturers were disclosed.

In March 2017, WikiLeaks disclosed that the CIA has tools for hacking IoT devices, such as smart TVs, to remotely record conversations in hotel or conference rooms—opening a Pandora's box of potential privacy issues.[7]

In May 2017, the National Health Service (NHS) in the UK was left vulnerable to the WannaCry virus, which took down IT systems at many of NHS organizations including about 30 hospital trusts, and as many 70,000 NHS devices. Locked out of systems by the file-encrypting malware, many NHS offices had to resort to pen and paper and thousands of operations and appointments were cancelled.[8]

The research shows it takes personal experience to drive action. More specifically, companies that have experienced a security breach are actively taking or have completed more steps to mitigate risks compared to those that have not experienced a breach.

Breaches also lead companies to change their approach. More specifically, tapping outside resources is more common among those that have experienced a breach.

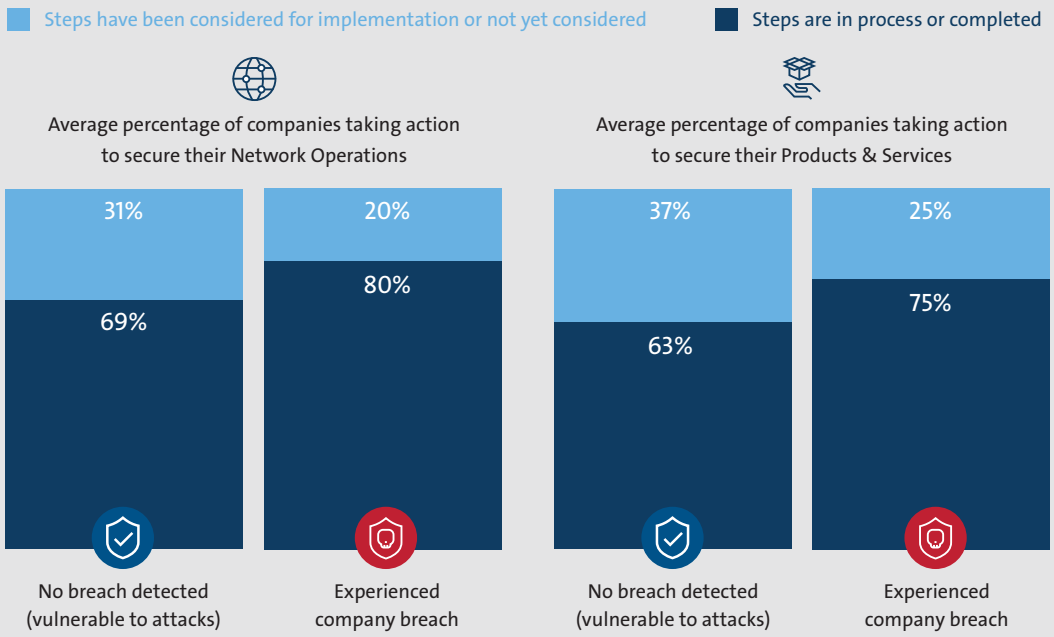
73%

of companies that have experienced a breach have hired outside resources.

Only 14%

of companies have instituted a formal audit process to help understand whether their devices are secure and how many devices they have.[10]

Steps taken to mitigate risk when it comes to Network Operations vs. Products and Services.



Personal experience trumps complacency

Lack of proactive action is a common human behavior characterized by normalcy bias—people naturally underestimate the possibility of a disaster and its potential impact. It's the same reason that people who live in an area known for flooding will often neglect to buy flood insurance. In fact, about 70 percent of people reportedly display normalcy bias in disasters.[9]

Individuals often assume that because they have never personally experienced a disaster, they never will. In cybersecurity terms, this typically results in situations where people fail to adequately prepare for, or even consider, the possibility of being victim of a data breach.

Addressing hidden weaknesses

Security vulnerabilities are actively being addressed by device developers, but concerns remain. For companies across industries, one of the more damaging but less often identified causes of cybersecurity breaches can be found in third-party software purchased or downloaded for use in internal systems and operations or for integration into finished goods.

Unfortunately, while third-party software components can help to increase development productivity and even result in better product quality, their expansive use has also introduced new cybersecurity risks, leaving critical infrastructure industries even more vulnerable to cyberattacks.

Without adequate systems and procedures in place to evaluate and control third-party software and components sourced from the software supply chain, organizations may unknowingly use or integrate software into operational systems or end products with insufficiently robust security that can be easily hacked or otherwise compromised.

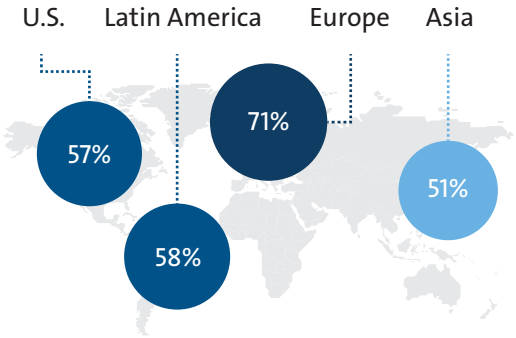
For organizations in critical infrastructure industries, these and other risk factors heighten the importance of evaluating software supply chain vulnerabilities, and developing and implementing programs that can help reduce risks connected with third-party software.

Regulatory standards: Seeking clarity in a sea of complexity

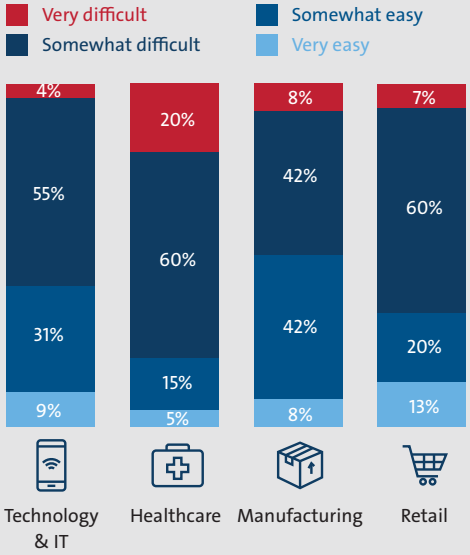
The guidance of governments and their corresponding legislative assemblies can help create a secure IoT ecosystem and framework. Nevertheless, while IoT security standards are welcomed and much needed, compliance can be challenging.

In our survey, the majority of organizations (59 percent) find compliance with security regulations difficult. Compliance difficulty was notably higher in Europe (71%), which coincides with a lower level of familiarity with compliance standards—only 39 percent (very familiar) versus 66 percent in the United States.

Percentage of companies finding compliance regulations challenging.



Perception of compliance difficulty varies within industry sectors.



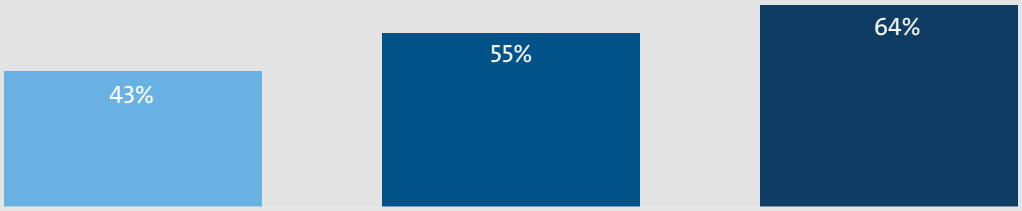
The percentage of companies finding compliance difficult was notably higher in the health care and retail sectors, at 80 percent and 67 percent respectively. The manufacturing sector finds compliance easier than other industries, with only half reporting it as difficult.

Role also impacts perception of difficultly. That is, the closer one is to the compliance process (tactics and implementation), the more challenging it is.

Only about half are "very familiar" with their country's standards for securing connected devices. Slightly higher familiarity with industry over country standards may suggest these are prioritized.

Perception of difficulty differs between management roles.

The closer a manager is to dealing with compliance tactics and implementation (e.d., directors vs. C-suite), the greater the perception of difficulty



Combatting the rise of automated attacks

The rise of botnets and other automated and distributed attacks create a threat that reaches beyond any single company or sector. As the connected economy grows, so does the potential for these types of attacks to create a variety of digital hazards.

To address these threats, the U.S. government is working with stakeholders on a set of goals and actions designed to increase ecosystem resilience. As a guiding framework, the U.S. Departments of Commerce and Homeland Security have released a report designed to promote action against these threats. The report, "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats", responds to a May 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[11]

As part of a private sector effort, the Council to Secure the Digital Economy (CSDE) has released its 2018 International Anti-Botnet Guide, which offers a set of voluntary baseline practices and advanced capabilities. In response to its concerns about too much regulation, the CSDE advised that "dynamic, flexible solutions that are informed by voluntary consensus standards, driven by market demands, and implemented by stakeholders are the better answer to these evolving systemic challenges."[12]

Security standards help shape IoT future

To balance growing IoT safety concerns and challenges with the rapid pace of innovation, UL has developed a Cybersecurity Assurance Program (CAP) in accordance with its new UL 2900 series of Standards. CAP aims to provide a set of requirements that manufacturers of network-connectable products can use voluntarily to establish a baseline of protection against vulnerabilities and software weaknesses.

UL is also contributing and leading the development of a number of new and emerging cybersecurity/risk management standards and programs including:

- ISO 18013 Guidelines for the design format and data content of an ISO-compliant driving license (IDL) in regard to both visual human-readable features and ISO machine-readable technologies.
- FIPS 140 U.S. government computer security standards that specify requirements for cryptography modules that include both hardware and software components.
- ISO 2434 Cybersecurity recommendations in mobility (including connected and autonomous vehicles).
- UL 5500 UL standard that cover remote software updates, as well hardware compatibility necessary for safety of the remote software update.

While there is no silver bullet to tackle manufacturers' cybersecurity needs, these guidelines and recommendations are designed to evolve and incorporate additional technical criteria as the security needs in the marketplace change.

Spending on IoT security gains momentum

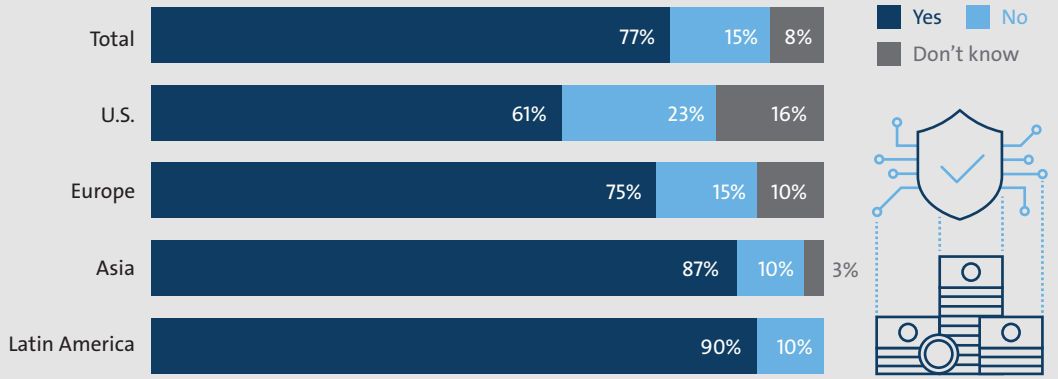
Organizations across industry sectors are quickly realizing that IoT security is not something that can be ignored or overlooked. Each new connected device represents another strike channel for organizations and it only takes a single device to corrupt an entire ecosystem and wreak havoc on business operations.

To fully capitalize on the immense benefits of the IoT, organizations must first establish a solid security foundation. Smart, strategic investments in IoT security will play a central role in this effort.

Our survey shows that companies continue to invest in IoT security. In fact, most companies (77 percent), plan to increase spending in IoT security over the next five years. The likelihood to increase spending were notably higher from respondents in Asia and Latin America regions, coming in at 87 percent and 90 percent respectively.

Cybersecurity planning spending increases were notably higher in the healthcare and retail sectors, at 85 percent and 83 percent, respectively.

Percentage planning to increase spending on IoT cybersecurity over the next 5 years

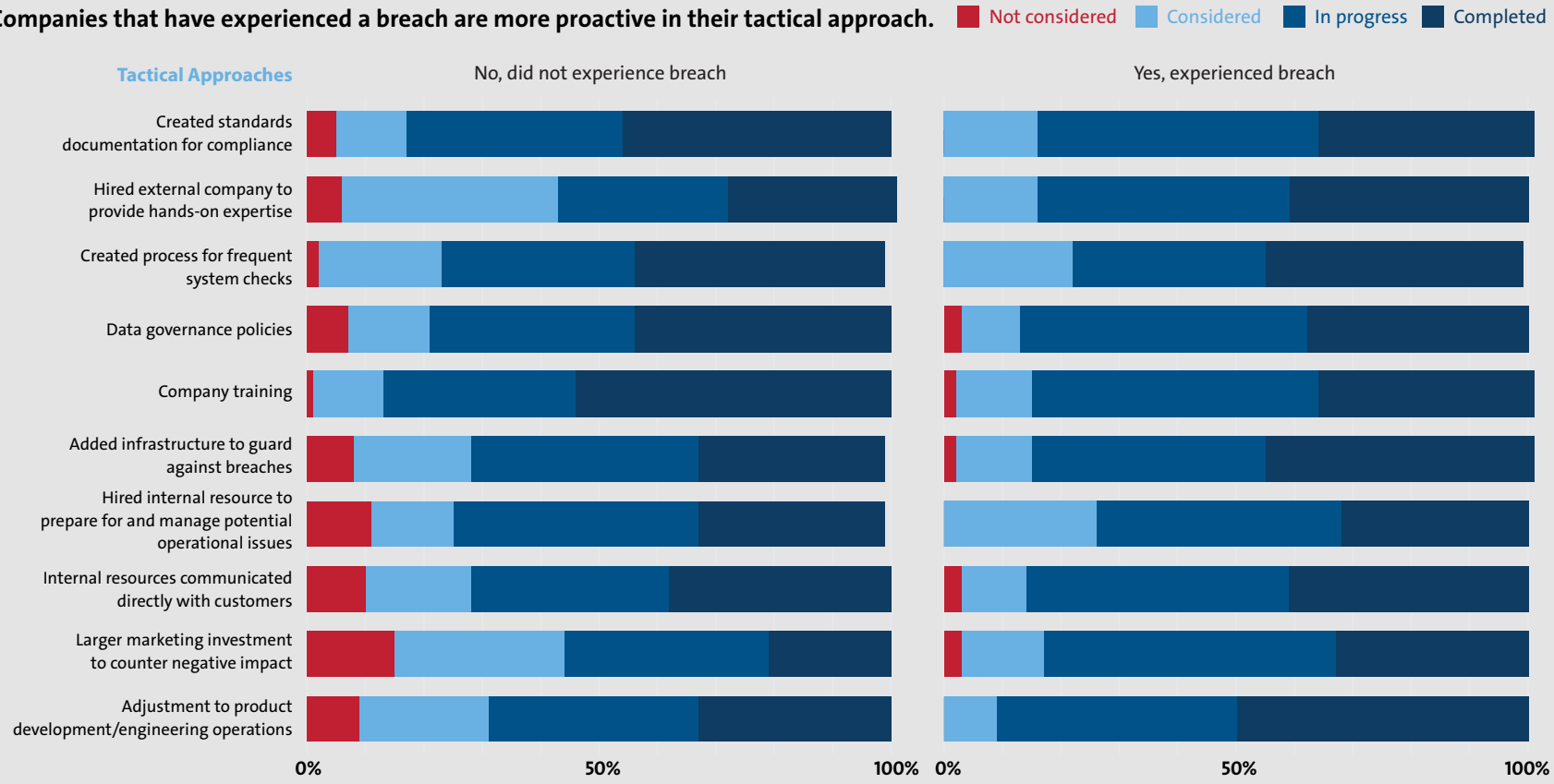


Incidents prompt action

Organizations are implementing an array of tactics to address IoT security concerns, with different strategies for those that have experienced a security breach versus those that have not. For companies that have experienced a breach, a range of tactics were reported in progress or already completed.

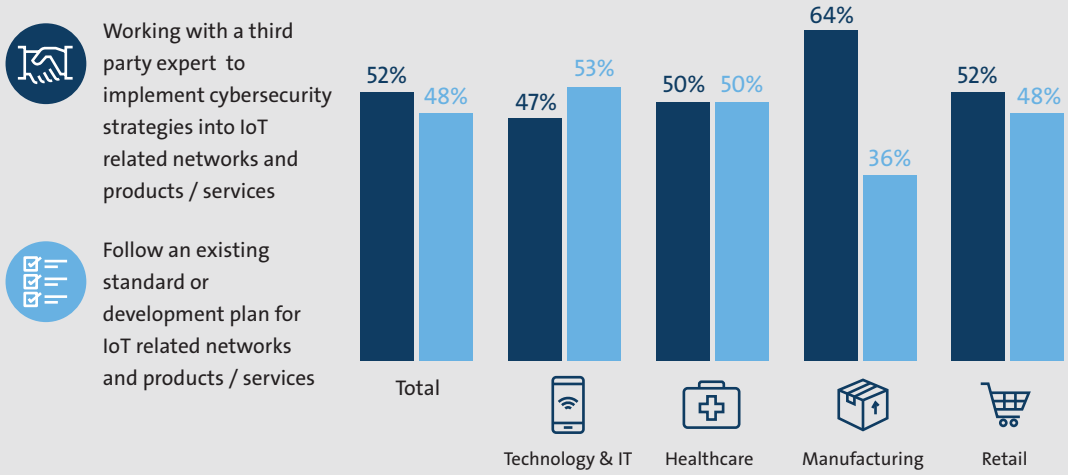
The potential of IoT technologies is reflected in projections of future IoT market revenue and growth. According to one estimate, the global IoT market will grow from $157B in 2016 to **$457B by 2020**, attaining a Compound Annual Growth Rate (CAGR) of 28.5 percent.[13]

Companies that have experienced a breach are more proactive in their tactical approach.



When it comes to implementing a new IoT security plan, 52 percent of companies plan to work with a third-party expert. This number was notably higher for respondents in the manufacturing sector (64 percent). The top reasons to consider a third-party expert were: “wider range of expertise” and “easier regulatory compliance”.

Companies in the manufacturing sector are more likely to tap outside resources.



89%

of respondents plan to introduce new products or services that address risks within the next 5 years. 62 percent indicated they are planning to do so within the next year.

19%

of companies plan to invest more than $100 million over the next five years on securing IoT products and services. 40 percent planned to invest $20 to $100 million.

52%

of companies plan to work with a third-party expert to implement new IoT security plans. The top reasons to consider a third-party expert were: “wider range of expertise” and “easier regulatory compliance.”

Seeking guidance on regulatory compliance

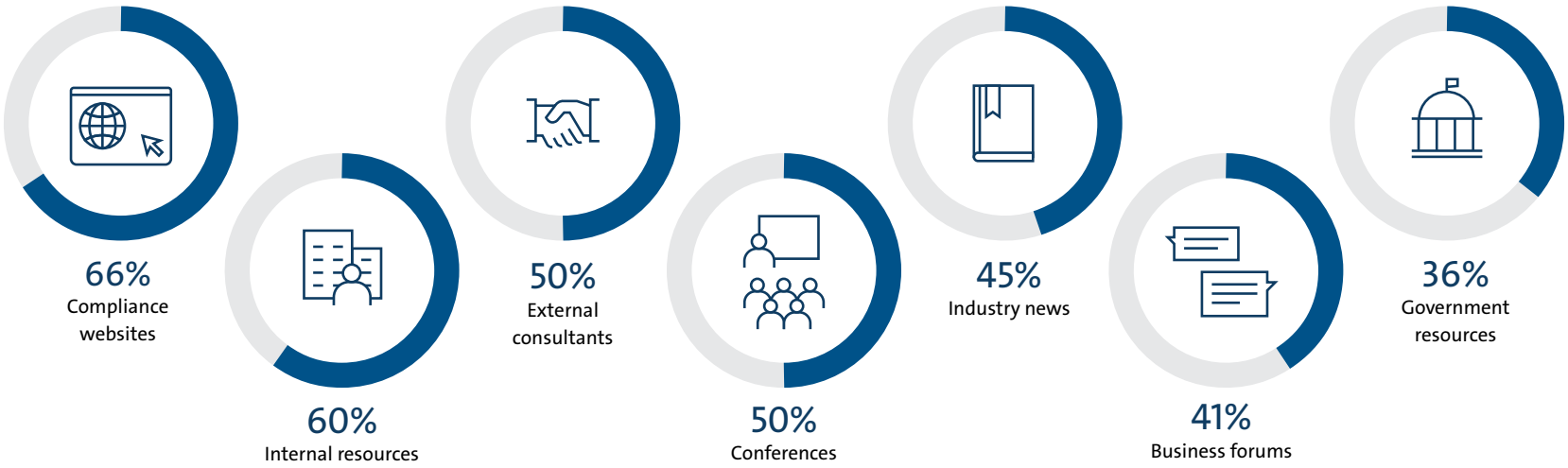
To stay informed on today's shifting regulatory environment, companies rely on a mix of resources. Compliance websites topped the list, followed by internal resources and external expertise.

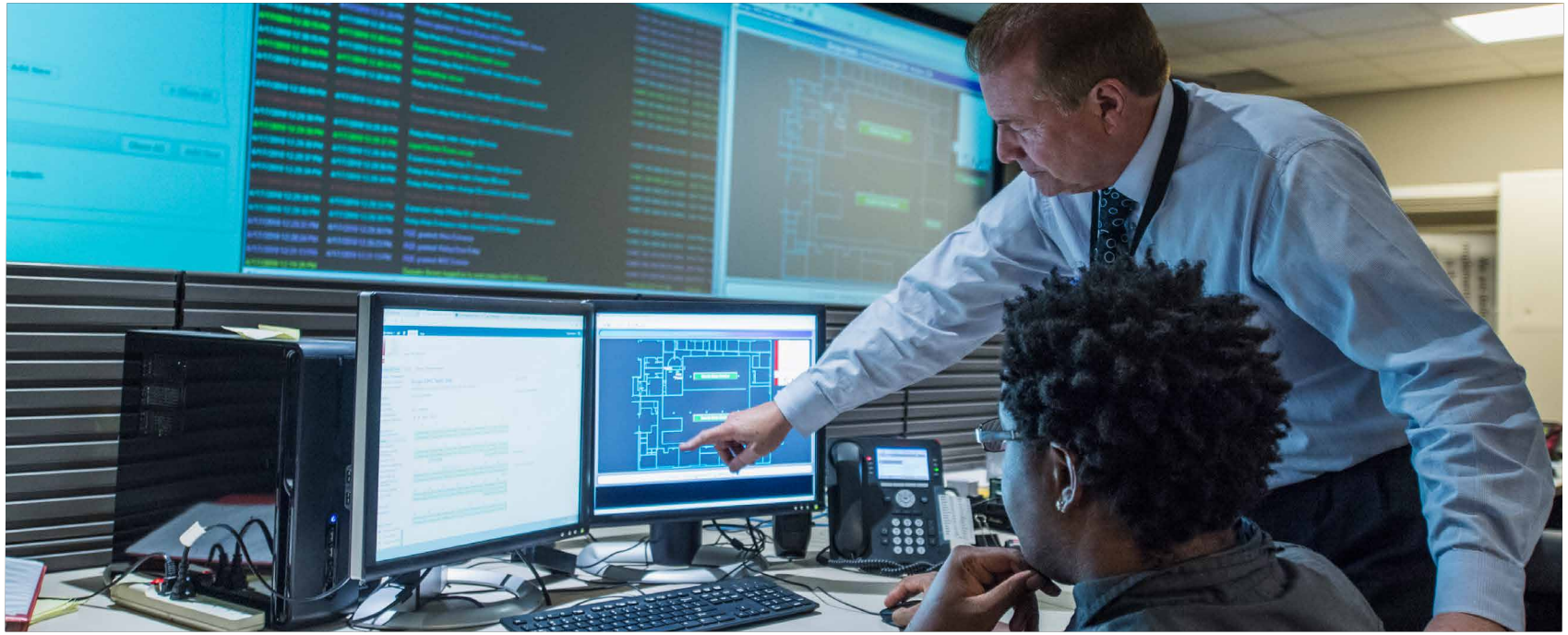
Government resources were cited by respondents as the least utilized tool for compliance guidance and support. While companies plan to use government resources, its low ranking may emphasize a tendency to prioritize industry compliance standards.

According to Gartner, IoT security spending will reach **$840 billion** by 2020[14]. At the same time, more than 25 percent of identified attacks on enterprises will involve IoT systems, stimulating companies to further increase their budgets for IoT security.

Companies utilize a range of compliance tracking tools.

Resources currently employed for compliance training





Effective security: The cornerstone to IoT success

The IoT presents a world of opportunities and challenges for businesses across industries. On one hand, it offers a diverse and personalized platform for customer engagement and operational efficiency. On the flipside, many elements are enormously complex, which heightens the risk of pushing customers away when safeguards fail. Finding that elusive balance between innovation and protection will be a major differentiating factor for customer-centric brands in the coming years.

Security is essential for the safe and responsible operation of IoT devices. In fact, it the foundational enabler of IoT. As such, it is vital for companies to establish robust mitigation strategies that can effectively identify threats and thwart attacks as they arise. Until proper safeguards are in place, IoT devices will continue to suffer under the weight of vulnerabilities.

While building an effective IoT security framework is a long-term process, organizations cannot afford to hesitate. Tactics and strategies are being formulated today, and forward-thinking organizations are already putting their plans into action now to ensure that their IoT ecosystems are able to effectively embrace and support the rapid escalation of connected “things.”

About UL

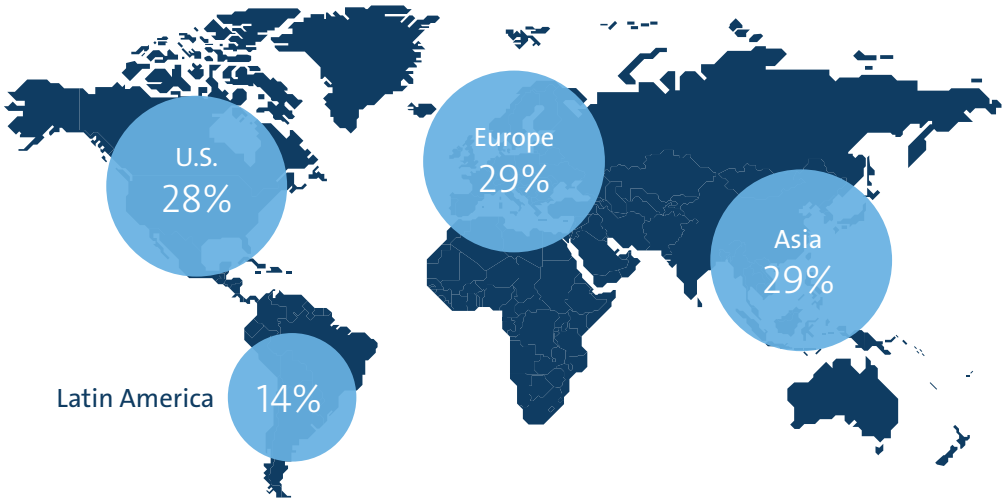
Around the globe, UL works to help customers, purchasers and policymakers navigate market risk and complexity. UL enables trust and vital end-to-end security designed for our interconnected world. We possess a unique expertise in developing security frameworks, structuring security programs for IT and interconnected ecosystems. We enable businesses to implement innovations without compromising on security, helping to maintain customer trust while increasing market access.

As an IT Industry partner and collaborator, UL aims to create standards and policies that will help ensure the safe and secure adoption of new connected technologies. UL is prepared to deliver services, solutions and education to help enterprises strengthen their brands. We invite you to take advantage of our leading-edge insights and domain experts to position your brand for long-term, sustainable success.

About the study

The findings in this report are based on a survey of 349 respondents from the United States, Europe, Asia and Latin America. Survey respondents represent senior managers, directors and IoT decision-makers and above who are responsible for coordination and management of IoT security practices and initiatives within their respective organizations.

Country breakdown



For more information, visit UL.com/insights.

Sources

1. The Internet of Things: A movement, Not a Market, IHS Markit, Oct. 2017
2. State of IoT Security, Research Report, Gemalto, 2017
3. Tales of Dirty Deeds and Unscrupulous Activities, 2018 Data Breach Investigations Report (DBIR), Verizon, 2018
4. Why Security Breaches Go Unnoticed for Months, 451 Research, June 2017
5. DDoS attack that disrupted internet was largest of its kind in history, experts say, The Guardian, 2016
6. Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON, IT World, 2016
7. WikiLeaks discloses details of CIA hacking IoT, mobile devices, Internet of Business, 2016
8. Worldwide ransomware hack hits hospitals, phone companies, CNET, May, 2017
9. The frozen calm of normalcy bias, Gizmodo, retrieved, May 2017
10. Second Cybersecurity Insights Report, Exploring IoT Security, AT&T, 2016
11. Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats—A Report to the President, The U.S. Secretary of Commerce and The Secretary of Homeland Security, May, 2018
12. International Anti-Botnet Guide, the Council to Secure the Digital Economy (CSDE), 2018
13. Market Pulse Report, Internet of Things (IoT), GrowthEnabler, 2017
14. Forecast: IoT Security, Worldwide, Gartner, 2016.

UL.com