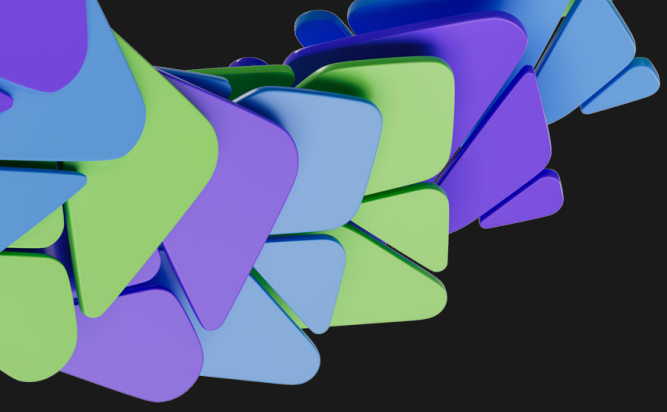
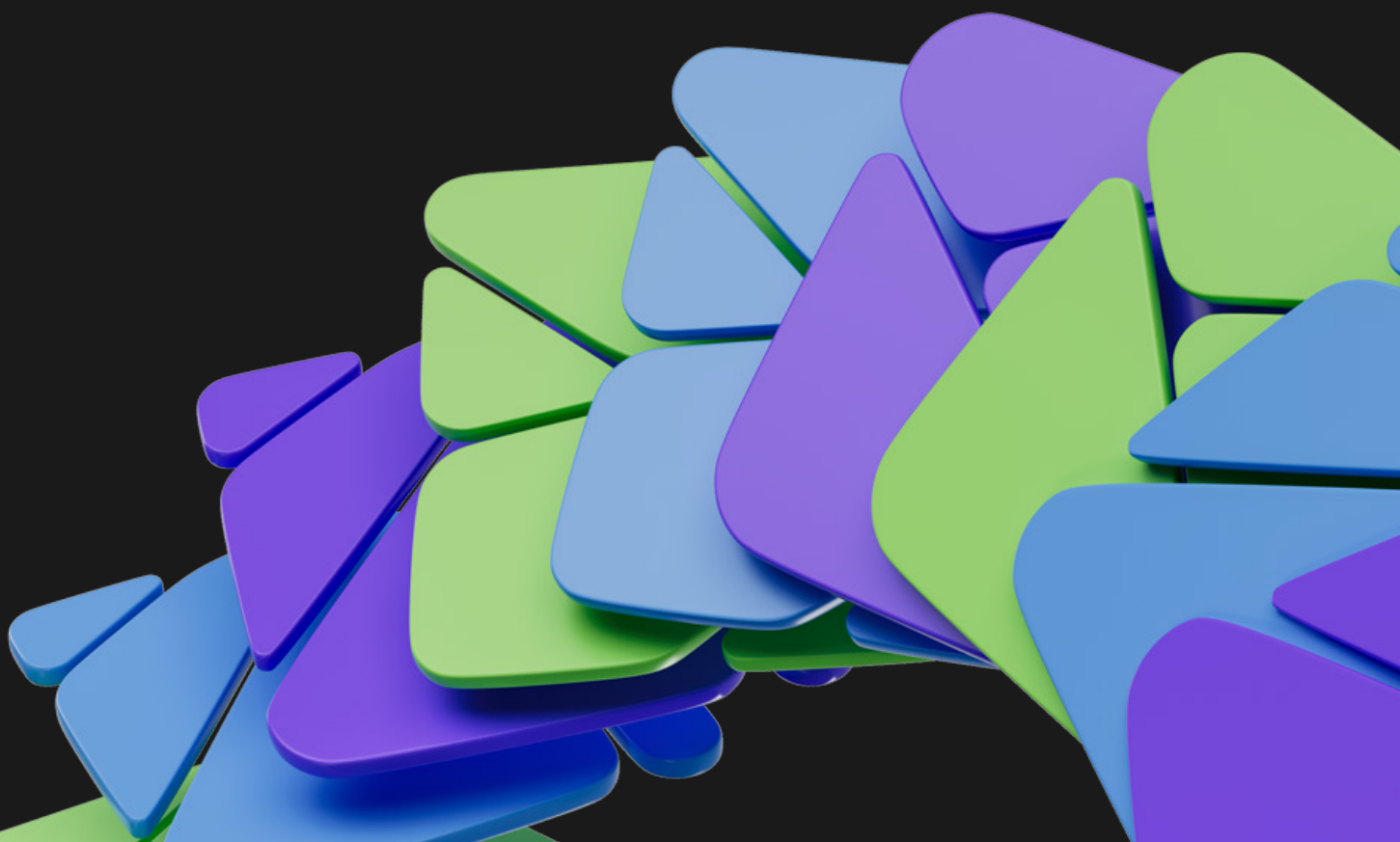
Digital Trust in a Connected World:

Navigating the State of IoT Security

KEYFACTOR

VansonBourne





Executive summary

In today's interconnected world, the Internet of Things (IoT) has emerged as a groundbreaking phenomenon. It promises to revolutionize industries, enhance efficiencies, and transform the daily experiences of businesses.

However, as IoT continues its rapid expansion and becomes increasingly integrated into business activity, the need for digital trust becomes a chief concern. Digital trust is quickly becoming both the framework and backbone of modern technological integrations and inventions. From remotely updating the software in smart cars to ensuring life-saving pacemakers are designed safely and securely, it all starts with a foundation of digital trust.

The undeniable benefits of IoT and connected device technology, such as helping to digitize business models and provide insights into operations, cannot overshadow the potential risks and vulnerabilities. From data breaches and privacy invasion to manipulation of critical infrastructure, the security of IoT devices demands attention and improvements. With digital trust, companies can build long-term relationships in the connected world in innovative ways — without it they face multiple consequences.

To better understand how organizations are addressing the rising challenges brought by IoT, we analyzed survey responses from 1,200 individuals across North America, EMEA, and APAC. These include OEMs (original equipment manufacturers) and those who are using and operating connected devices within their organization. Please see "Research methodology" on pages 52–53 for additional details on the audiences surveyed.

In this report we will explore the challenges faced in securing IoT and connected products, delving into the potential consequences of inadequate security measures. We will examine key factors contributing to the vulnerability of organizations using IoT and connected devices, including the rapid proliferation of connected devices, the cost of inadequate cyber defense, and the complexity of where liability lies for successful cyber breaches.

Moreover, we will discuss the pressing need for improvements in IoT security and the current initiatives taken by professionals working with IoT and connected devices in their day-to-day activities to address these challenges. We will delve into how organizations are managing their digital identities, exploring how PKI solutions and certificate lifecycle automation platforms are sought-after solutions for success. We will also highlight the importance of user awareness and education in empowering individuals to make informed decisions regarding their connected IoT device security.

Additionally, we will explore two specific organization types:

- Looking in depth at **OEMs for IoT and connected devices**; what methods and priorities are they leveraging for optimal security for their IoT and connected products, and their specific challenges surrounding cyber breaches and the costs they are facing
- Delving deeper into **organizations that use or operate IoT and connected devices**; considering their pain points and needs for additional support

Ultimately, the aim of this report is to shed light on the need for heightened security in IoT and connected products used in businesses and to provide insights into the efforts being made to tackle the associated challenges. It equips readers with a deeper understanding of the vulnerabilities in IoT and connected devices and the measures required to enhance their security, to ensure the long-term viability and success of this transformative technology within their enterprises.

SUBJECT MATTER EXPERT

Ellen Boehm
SVP, IoT Strategies and Operations

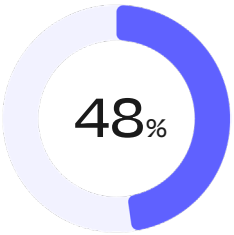
Keyfactor

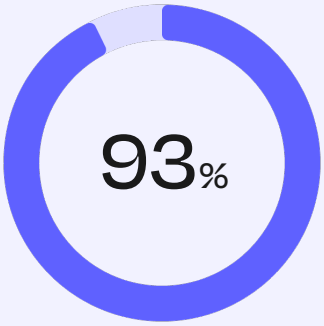
Contents

Key findings

The key findings described here are based on the research data compiled by Vanson Bourne.

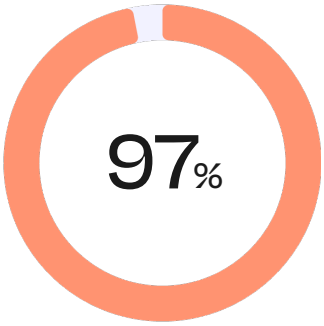
Forty-eight percent believe that the manufacturer of IoT or connected devices should be *at least mostly* responsible for cyber breaches on their products.





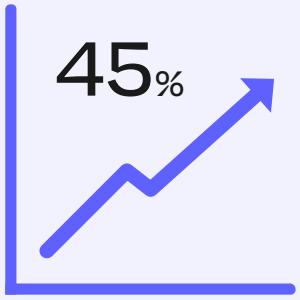
of organizations are using PKI solutions to issue digital identities and/or manage certificates — with most using a hybrid of active third-party and internal solutions.

Yet,



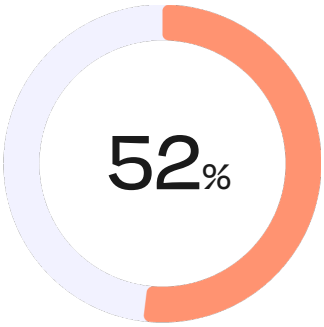
of organizations face challenges in securing their IoT and connected products to some degree — **which begs the question, are they securing them in the right way or are they leveraging the wrong tools?**

Over a third (37%) report that significant improvement is needed in the security of the IoT/ connected products in their organization, with 60% reporting that a little improvement is needed.



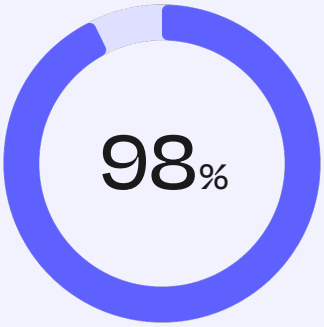
Budgets for IoT device security are increasing year over year, with an anticipated **increase of 45% in the next five years.**

However,



of their budget is at risk of being diverted to cover the cost of successful cyber breaches on their IoT and connected products.

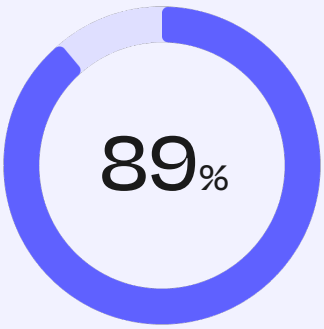
On average, there has been a 20% increase in the number of IoT and connected products used by organizations in the past three years.



of organizations have experienced certificate outages in the last 12 months.

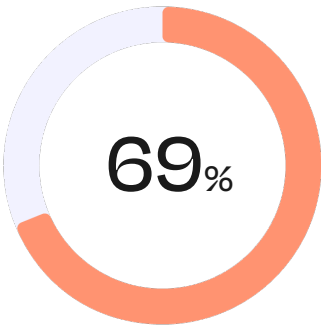
The total average cost to OEM organizations for certificate outages on their manufacturing lines in the last 12 months was over

$2.25 million.
(USD)



of organizations that operate and use IoT and connected products have faced cyber attacks in the past twelve months at an average cost of a quarter million dollars.

and,



of organizations using or operating IoT devices have seen an increase in cyber attacks on their IoT devices over the past three years.

On top of covering the cost of successful cyber breaches and certificate outages, the financial burden has potential to become insurmountable – *it's vital to invest today, to avoid paying tomorrow.*

Over half (56%) agree that their organization doesn't have the proper awareness and expertise to prepare for cybersecurity attacks through IoT devices — organizations need support and guidance to move forward.

Organizations don't necessarily understand what being "fully" protected from cyber attacks entails — with 43% believing they are as protected as they can be.

Ready to learn more?

The complete findings described below are based on the research data compiled by Vanson Bourne.

Looking for a product?

Find out how to create and maintain trust in your IoT products by protecting and managing their identities at scale with Keyfactor Command for IoT.

View datasheet ↗

Section 1

The state of security in IoT and connected devices

In this section, we explore the state of security and IoT and connected devices. We have organized topics in the following order:

1. Security compliance vs security complacency
2. Growing demand for external PKI solutions
3. Vendor demand

Security compliance vs security complacency

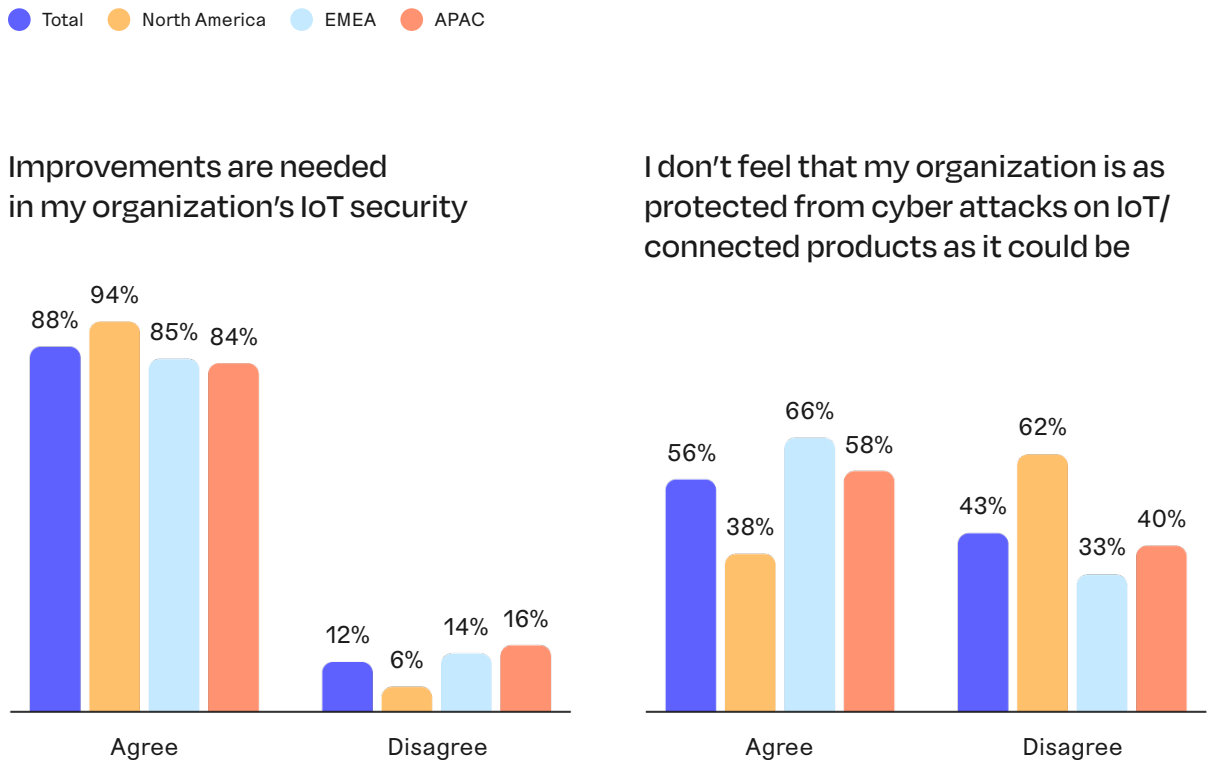
As organizations seek to harness the power of IoT and connected devices to streamline operations and gain a competitive edge, failing to comprehend the immense vulnerability that such connectivity brings can be devastating to an organization's success. Whilst organizations may tout their security measures and reassure stakeholders, the truth remains that there are shortcomings in the protective strategies employed.

Many organizations agree that overall improvements are needed in the security of IoT and connected products — ranging from a little improvement (60%) to significant improvement (37%), but crucially, very few report that no improvements are needed which suggests there is an awareness that the current level of protection is insufficient for the ever-changing nature of digital threats.

Figure 1

To what extent do you agree or disagree with the following statements?

Showing the combination of "strongly" and "slightly" responses. Split by region, omitting some answer options.



However, there is a marked sense of complacency with product security regionally for those that operate and use IoT and connected devices. Demonstrating this, almost all organizations in North America (94%) agree that improvements are needed in their organization's IoT security, but almost two thirds (62%) believe they are as protected as they could be from cyber attacks on IoT and connected products. This is creating a juxtaposition; organizations believing they are as protected as possible but also needing further improvements. It's suggesting that some businesses have reached a level of protection where they feel satisfied but haven't further investigated or sought solutions to really delve into what "full" protection might be.

And similarly, in the EMEA and APAC regions, a minority of organizations (33% and 40% respectively) still report their belief of being as protected as possible. It's clear that further education is needed on what being "fully protected" in terms of IoT and connected device security means, with organizations perhaps unaware of what other stronger options are out there.

Growing demand for external PKI solutions

The demand for PKI solutions is evident, with almost all (93%) surveyed organizations reporting that they have one in place to issue digital identities or manage certificates. Largely being driven by the US with the largest respondent pool, the UK is lagging behind with only three quarters of organizations having PKI in place.

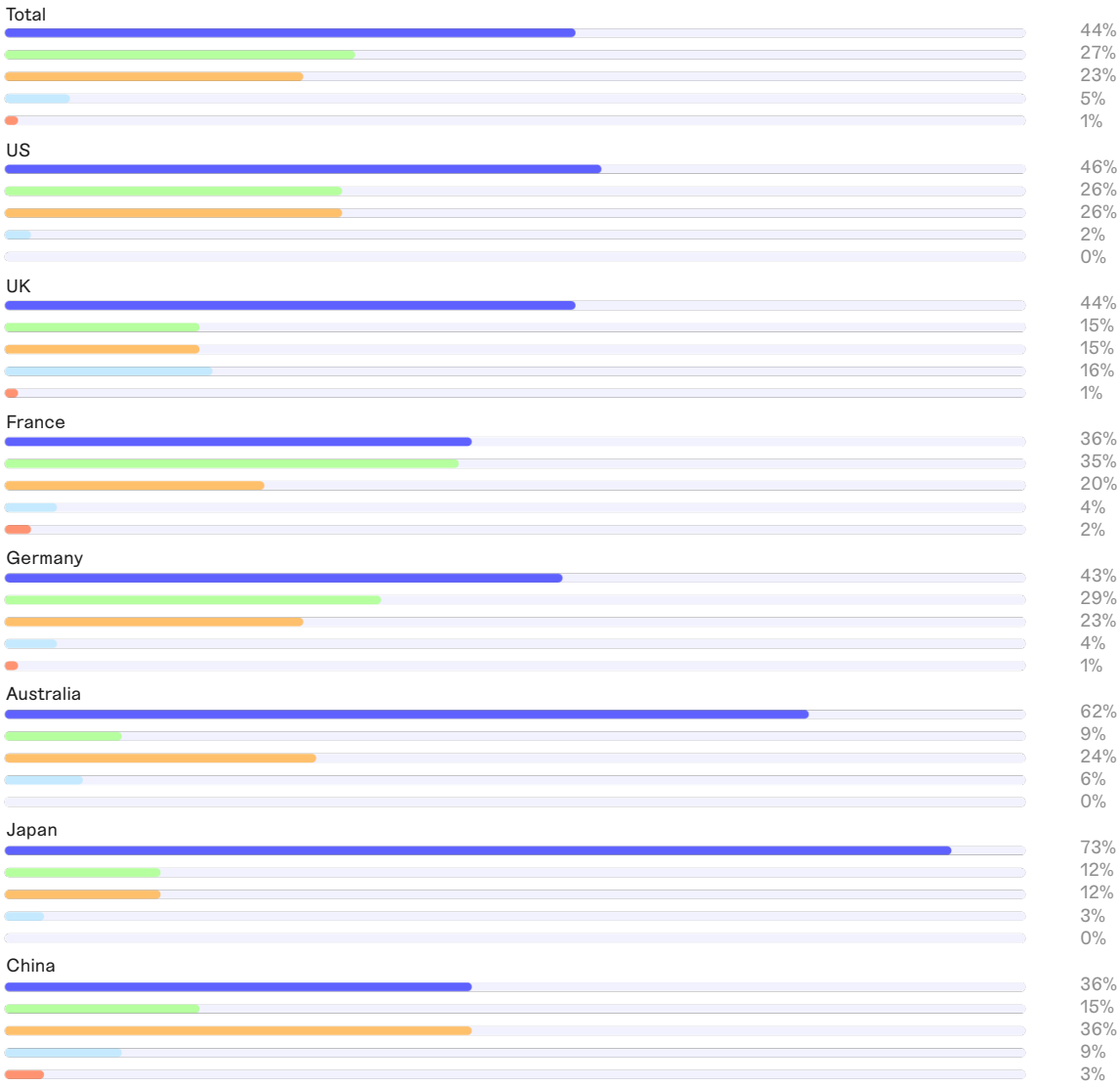
Third-party vendors are at the forefront of this, with many organizations turning to vendor support to manage this functionality. In most cases globally, active third-party solutions are paired with internal solutions to effectively manage these elements on their IoT and IIoT (Industrial IoT) devices, showing a keen uptake of external support. With outsourcing providing benefits including the freeing of internal resources, support, and maintenance over time, and cost efficiencies when considering the total cost of ownership, it's no surprise that one in two (49%) organizations are using third-party suppliers to manage digital identities (certificates and keys) of IoT or connected products.

Considering that most organizations report that improvements are needed in their IoT and connected product security [page 11], working with vendors to either support their internal PKI solutions or to entirely outsource the solution seems to be a logical step to provide additional security to devices. With 4 in 10 organizations that operate and use IoT and connected products reporting that they strongly agree they would benefit from using a PKI to issue digital identities on the IoT and IIoT devices in their environment, there is an opportunity to partner with a vendor for their PKI solution and experience the advantages that it offers.

Figure 2

Is your organization utilizing a Public Key Infrastructure (PKI) solution to issue digital identities and/ or manage certificates on the IoT and IIoT (Industrial IoT) devices in your environment / on the IoT devices that you design/ manufacture?

Split by country, omitting some answer options.



Vendor demand

With IoT and connected product usage increasing in the past three years [page 39], organizations are seeking further support with the management of these devices.

Figure 3

Why does your organization use third parties to manage the digital identities of its IoT/ connected products?

Asked to respondents that use third parties to manage the certificate lifecycle of its IoT devices. Split by respondent type, omitting some answer options.

When experiencing a significant increase in device numbers or usage, organizations are more likely to be managing their digital identities through third parties compared to those that have seen their product usage stay the same or decrease. Vendor support being more significantly sought as device numbers increase demonstrates that organizations are struggling to manage this growth. With maintaining a high level of security for their devices of upmost importance, having a dedicated supplier to manage the devices and assume some responsibility for security elements will ease the minds of those organizations.

The demand for third-party vendors is clear, however there are variances in what organizations are seeking from their suppliers. Typically, flexibility, cost saving benefits, and having full visibility of certificates in one place are among the top priorities.

89%

of users/operators agree their organization would benefit from utilizing a certificate lifecycle automation platform to manage certificates

However, organizations' size and function when thinking of IoT and connected products have differing priorities for vendors. Those that operate and use IoT and connected products find flexibility of more importance, and cost-saving benefits are of primary importance for OEM organizations. The key areas that each organization type is seeking from their vendors indicates particular pain points that they are experiencing and therefore why they are seeking this externally to ease their frustrations.

46%

of users/operators in smaller organizations (under 5,000 employees) **strongly** agree their organization would benefit from utilizing a certificate lifecycle automation platform to manage certificates

Of similar popularity is utilizing vendors for a certificate lifecycle automation platform to manage certificates, with almost 9 in 10 agreeing that they would benefit from using one. Smaller organizations (those with 500 to 4,999 employees) are more likely to **strongly** agree there are benefits to their organization using this platform, and this is shown in what they are seeking in external suppliers. As is often found with smaller organizations, they tend to experience internal workload concerns, and therefore are more likely to report associated challenges, such as time savings (36%) and reducing the internal workload (38%) as reasons for using third parties to help with digital identity management. This indicates that those with lower employee counts, and therefore likely lacking certain skills internally, benefit from having close assistance from external support.

Section 2

IoT and connected device security challenges

In this section, we examine the security challenges presented by IoT and connected devices. We have organized the topics in the following order:

1. Areas of challenge for organizations' IoT and connected product security
2. Security budgets: 2023 and beyond
3. The impact of industry standards and regulations
4. Cyber breach responsibility
5. But it depends on the breach?

Areas of challenge for organizations' IoT and connected product security

The constant-threat nature of IoT or connected product security is leaving organizations with many sizeable concerns and challenges, compounded by almost all organizations stating they face challenges in securing IoT/ connected products.

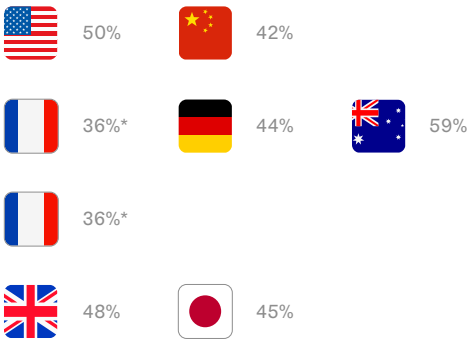
Figure 4

What challenges, if any, does your organization face when looking to secure the IoT devices that you design/ manufacture?

Omitting some answer options.

Top answers, by country

*joint top answers



97%

of organizations face challenges in securing IoT/ connected products

Those who haven't experienced any cyber attacks on their IoT and connected products in the past 12 months are more likely to say that they do not face any challenges in securing their products or those that they design and manufacture (22%) compared to those that have experienced attacks (2%) — there's a clear level of naivety among those who haven't experienced attacks. Those who have experienced attacks recognize the multi-faceted aspects of protecting their devices, and therefore are knowledgeable of what challenges occur because of this. We explore further the experiences of those that have experienced cyber attacks on pages 44-46.

However, despite what we have seen with the desire for vendor support, organizations are having to make a compromise. They are needing to use third-party devices as a necessity, and outsourcing their security elements is also becoming evidently more important. But, many (42%) don't have the visibility and transparency that they are craving, causing high levels of concern surrounding how protected these devices are (43%). This is generating an overall feeling of wariness of how organizations feel towards securing their IoT products, which needs to be overcome in order to fully realize a successful working partnership with vendors. Creating a trusting and open relationship with a vendor will provide clarity surrounding the security of devices, which will help to alleviate any feelings of concern.

Curiously, less than a third of organizations are feeling challenged by cost in relation to IoT and connected product security, which is a concern. Perhaps it is that organizations feel that cost is irrelevant, and they are recognizing that there is a need to put increasing budget towards securing their IoT and connected devices — seeing it as a non-negotiable element, and therefore it isn't viewed as a challenge. Or, cost is being pushed to the back of the list when it comes to thinking about concerns and challenges with IoT security. If organizations become complacent when it comes to putting money towards IoT product security, it elevates the risk of any cyber attack being successful. Regardless, organizations need to carefully consider the best way to invest in security for their connected products and ensure that this is of priority when setting budgets every year, to protect against the ever-increasing cyber threat on IoT devices — as we'll delve in to, on page 42.

Security budgets: 2023 and beyond

There is recognition that spending in the area of IoT and connected device security is imperative, with budgets expecting to increase year on year for the next five years. With a planned 45% increase in budgets for that time period, organizations are aware that they need to spend in this area to protect their organization's devices from threat. It's acknowledged that this investment is crucial and demonstrates that product security is being prioritized.

Figure 5

Please estimate how much budget your organization has for the security of IoT/ connected products this year?

Showing average budget.

▲ 45%

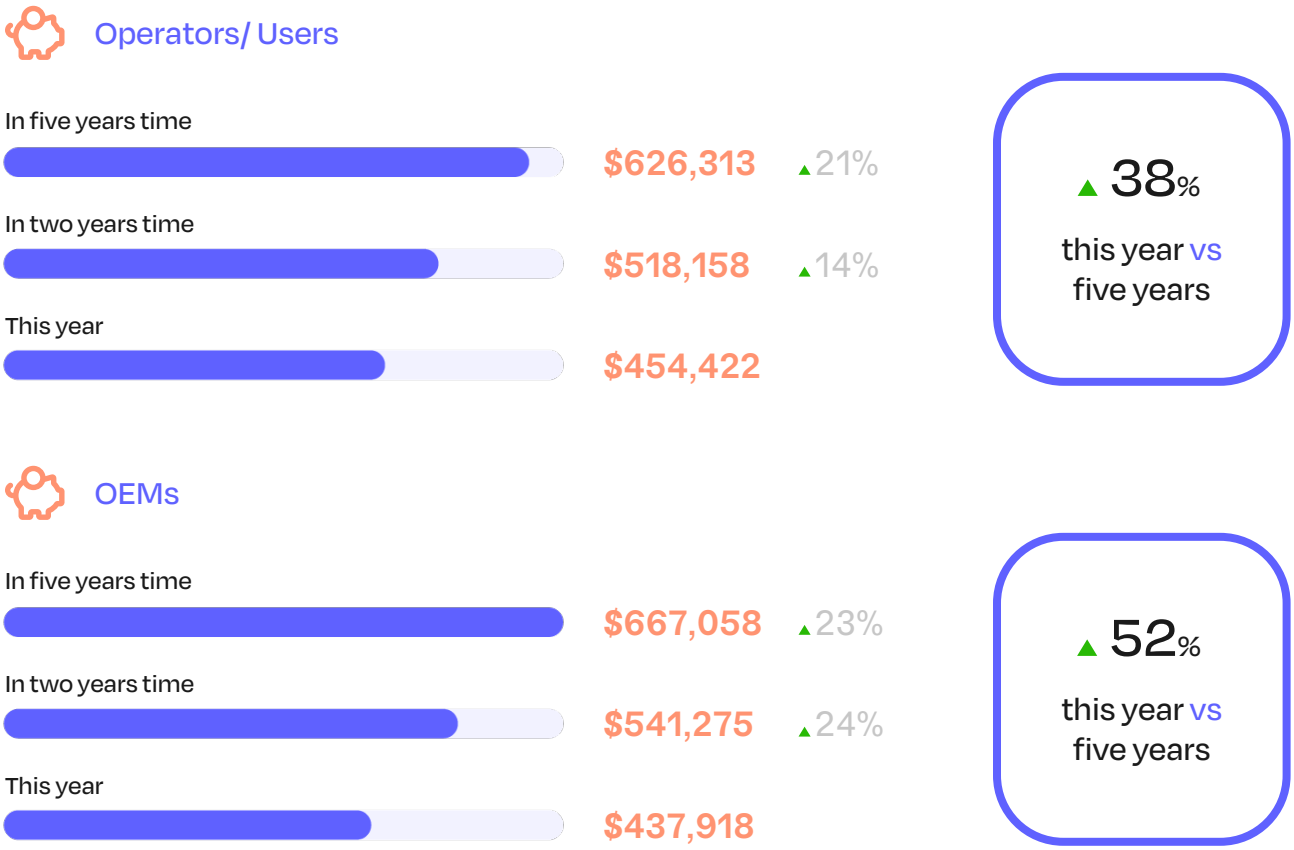
this year vs five years

Delving further into this, driving the year-on-year budget increase is OEM organizations, with an average increase of 52% in five years, showing a more substantial investment from the product manufacturer and design side in the security of their IoT and connected products. As we'll see on page 23, the liability for cyber breaches on connected products is a complex area and therefore OEM organizations are increasing their budget to help protect against responsibility.

Figure 6

Please estimate how much budget your organization has for the security of IoT/ connected products this year?

Showing average budget, split by respondent type.



Budget increases for operator/user organizations are also planned for, with an average increase of 38%, which is primarily due to an increase in cyber threat (45%) and an increase in the number of IoT and smart devices (45%). With the increase in device numbers likely raising the level of cyber threat that devices are exposed to, increasing budget is a rational step for organizations to take to ensure their devices are protected. Similarly, the more devices there are, the more potential there is for user error to cause cyber breaches, so organizations should be preparing their employees to follow procedures and updating security as frequently as possible.

Of note too is that a quarter of smaller organizations (26%) see their budget increasing due to experiencing certificate outages (in comparison to 9% of larger organizations), highlighting an area of struggle for smaller organizations and therefore something which vendor support could be sought to mitigate the need for increased budgets.

The impact of industry standards and regulations

Alongside budgetary concerns and challenges working with third-party suppliers and devices, organizations are also feeling under pressure when it comes to considering industry standards, compliance requirements, and regulations that they have to adhere to.

These elements are having a clear influence on the **development** of connected and IoT products, with conforming to standards and regulations having noticeable impacts on how organizations can advance in this area. Almost all (98%) organizations report that regulations do impact the development of IoT and connected products, which demonstrates how much these have influence over how a device can progress and be used within the market.

Vetting the supply chain for cybersecurity, being required to meet an industry cybersecurity standard in order to continue to sell products to the market, and adding personnel to more directly handle product security are reported as the top impacts of satisfying regulations and standards. Such standards include:

- Smart Home: Matter
- Automotive: UNECE 155/156, ISO 15118, ISO 21434
- Industrial: IEC 62443
- Multiple Industries: IEEE 802.1AR

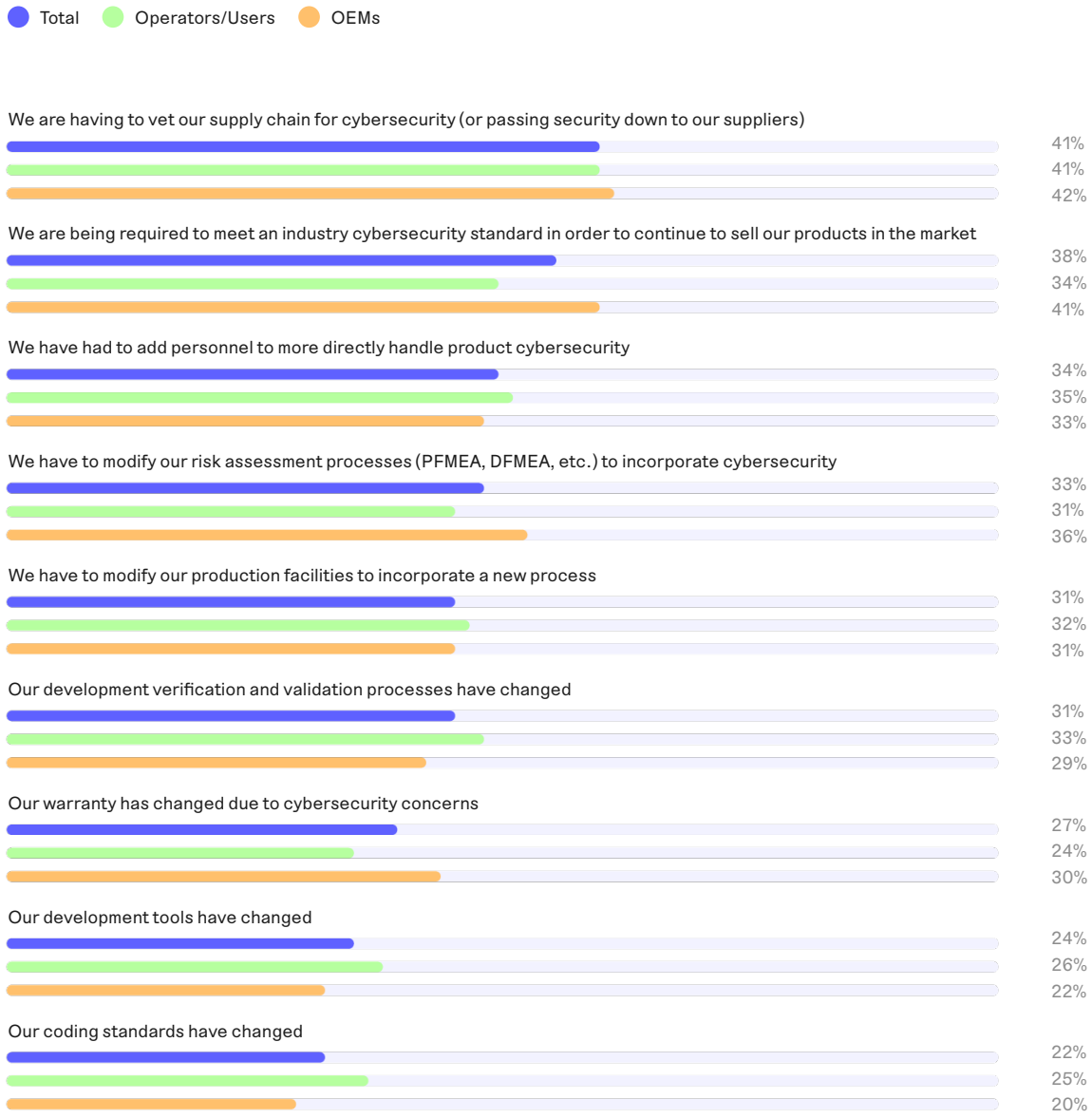
In particular, having to vet the supply chain for cybersecurity is a top impact of conforming amongst both organization types, and considering the costs of having inadequate cybersecurity for their products, it's no surprise that organizations are taking measures to ensure that all aspects of their supply chain are up to par. This ties to the potential lack of trust and transparency that there is with suppliers or vendors that organizations are working with [page 17] and is an area that will be beneficial to all involved — if improvements can be made.

And with almost 4 in 10 organizations that operate and use IoT and connected devices (38%) expecting their budget increases to be due to changes in government or other regulations that they will need to comply with, this dynamic area is something that organizations need to be prepared to keep pace with.

Figure 7

How are industry standards, compliance requirements, and regulations impacting the development of connected/ IoT products?

Split by respondent type, omitting some answer options.



Cyber breach responsibility

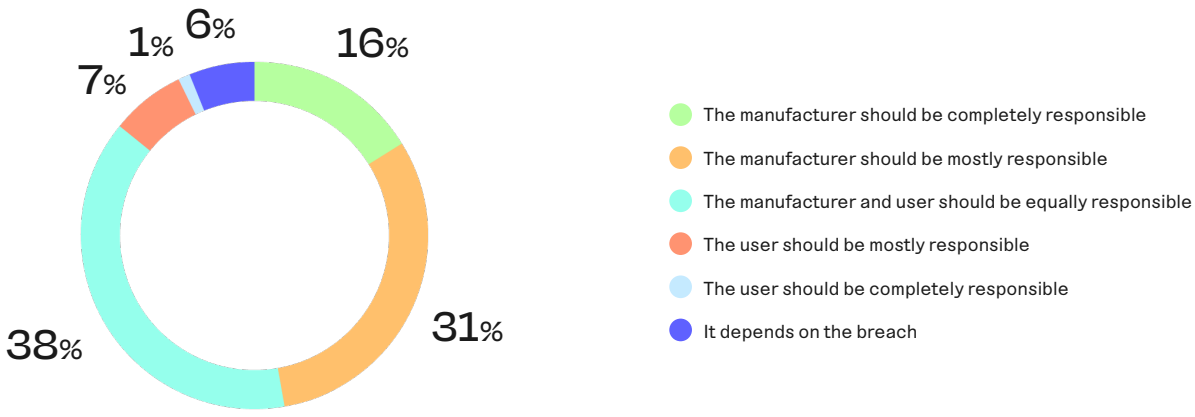
When cyber breaches occur, one of the foremost questions is, “Who is responsible for this?” With IoT and connected products, the answer is not always clear.

Almost half (48%) of respondents reported that the manufacturer of the IoT or connected product should be held **at least mostly** responsible for any cyber breaches, with this increasing to 53% in North America. This perhaps helps to explain the complacency spoken about on page 5. If organizations in North America on the whole believe that the manufacturer should take responsibility for any cyber breaches on their devices, then this could be why they feel they’re “fully” protected from cyber attacks.

Figure 8

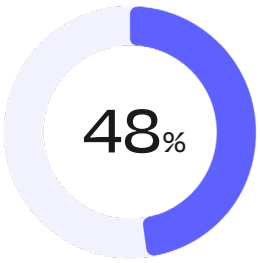
If an organization was to experience a cyber breach on its IoT/ connected products, who do you believe should be held responsible?

Omitting some answer options.



However, considering that 85% of organizations believe the manufacturer has responsibility at some level (whether total, most, or equal responsibility with users), this signifies that manufacturers should be prepared for a majority believing they have accountability when cyber breaches occur. This can lead to a negative association for manufacturers if a large-scale cyber breach occurs on one of their designed or manufactured products, so it's important to keep in mind the public **perception** of liability, as well as **actual** liability.

There is, however, a small proportion of respondents who believe that 'it depends on the breach' when it comes to being held responsible for breaches on IoT and connected devices. This is explored further on page 25.



believe the manufacturer should be *at least mostly* responsible

The manufacturer should be *at least mostly* responsible

North America	53%
EMEA	46%
APAC	41%

Split by region

But it depends on the breach?

When further probing respondents who believe there is a grey area with liability for cyber breaches (responding 'it depends on the breach'), many report that manufacturers have a responsibility to take actions such as releasing security patches and ensuring that any known vulnerabilities or flaws are covered. This would allow them to make certain that they have done all they can to protect the devices and provide confidence to users that they are protected.

However, there is also the view that manufacturers can only do so much. With end users being close to the products in their daily use, they must check for software updates and security patches that manufacturers release. They must also ensure that they are using the devices with the correct procedures and being alert to any possible cyber threat avenues; therefore continuous education for employees is critical. Without organizations being able to provide evidence of this, many believe that liability cannot be assumed upon the manufacturers and end users bear much of the responsibility.

Figure 9

In the previous question, you indicated that it would depend on the breach as to who is responsible for cyber breaches on organizations own IoT/ connected products. Please can you expand on the reasons for selecting this?

> “I think it is essential to know how an application is used before looking for the person responsible. This can come from improper use as well as from a flaw in production.”
>
> Operator/user

> “If a vulnerability is known and the manufacturer has not issued a patch then it would be the manufacturer’s fault. However if the user hasn’t deployed a patch in a timely fashion then it would [be] the user.”
>
> Operator/user

> “If the violation is due to negligence on the part of the user (non-compliance with the procedures for use or safety) it cannot be attributed to the manufacturer.”
>
> OEM

> “In reality, the liability incurred will mainly depend on the actual cause of this violation. This may be human error on the part of an employee or a software problem attributable to the manufacturer of the object in question.”
>
> Operator/user

> “Cyber security is a mixture of people, technology and process — the manufacturer can only be responsible for the technology aspects not the people or process related ones.”
>
> Operator/user

Ultimately, *there is an element of responsibility on both sides to ensure a device is “fully” protected, by both the manufacturers/designers and the operators/users*. Organizations need to be assured that they have taken the proper precautions and proactive steps so that the impact of cyber breaches are mitigated, or avoided altogether.

Section 3

OEM organizations

In this section, we dive deeper into insights from original equipment manufacturer (OEM) respondents. We have organized the topics in the following order:

1. OEM security priorities
2. The challenges faced by OEM organizations
3. Industry standards and regulation impacts
4. The true cost of certificate management
5. Lifetime responsibility of IoT and connected products

OEM security priorities

OEM organizations have a unique role in the security of IoT and connected devices. Developing products that are secure from the very foundation is crucial in safeguarding sensitive data, protecting user privacy and mitigating the risk of cyber attacks. However, achieving adequate security in IoT devices is far from straightforward. The diverse range of IoT applications, each with its own unique requirements and constraints, elevates the complexity of devising effective security protocols that can be universally applied.

To this point, OEMs have varying methods of securing connected devices and IoT products that they design and/or manufacture, and this varies by organization and by region. Only 1% are not looking to secure their devices, for the reason that the data isn't sensitive, therefore indicating that security is top of mind for OEM organizations and there are considerations in the methods they are utilizing. However, with an average of three methods used, are organizations doing as much as they can to protect their products?

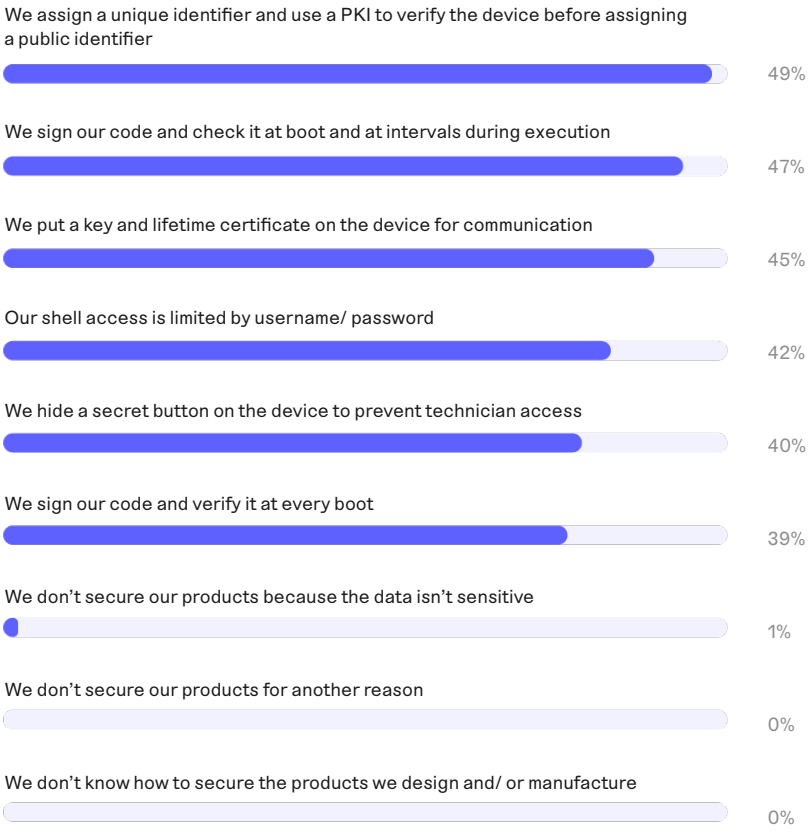
With OEM organizations withstanding the majority view that liability for cyber breaches on devices is directed towards them [page 23], the priority that these organizations place on security is fundamental to their success. 9 in 10 OEMs (91%) overall agree that they should prioritize security over overall functionality or product design, with 4 in 10 (42%) agreeing to this strongly, making it a fundamental part of the product and one that organizations should be, and are, prioritizing.

Further to this, 46% of OEM organizations strongly agree that securing brownfield on already deployed devices is of importance, and this vision is increasingly valuable considering the length of time to deploy brownfield IoT hardware or capabilities. Time is of the essence when security threats are identified, and therefore considering the quickest way to deliver solutions to their customers is imperative. Having this as a strategy that could provide quick relief to any possible cyber-threat could help OEM organizations reduce their liability and elevate their status as top manufacturers.

Figure 10

What methods do you utilize today to ensure the connected devices and IoT products you design and/ or manufacture are secure?

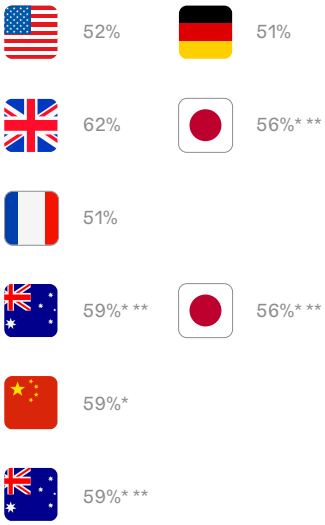
Respondents selected three answer options, on average. Omitting some answer options. Respondents' organizations are OEMs of IoT/ connected devices.



Top answers, by country

*joint top answers

** note low base sizes in Australia, Japan, and China



The challenges faced by OEM organizations

The challenges OEMs experience extend beyond technical aspects of connected device security. The lifecycle of IoT devices is extensive, encompassing various stages such as design, development, manufacturing, distribution, and ongoing updates. Each of these stages presents its own set of vulnerabilities and potential entry points for cyber threats. With these multifaceted challenges for OEM organizations, understanding the intricacies of these challenges can lay a solid foundation for implementing robust security measures and fortifying their products against potential vulnerabilities and threats — and there are considerations in the methods they are utilizing. However, with an average of three methods used, are organizations doing as much as they can to protect their products?

Almost all OEM organizations face challenges when considering the security of manufacturing/ production/ supply chain lines, and crave clarity and support surrounding best practices, equipment downtime, and the increase in potential of cyber attacks. And with additional challenges being a lack of skills or talent to manage complex structures (29%), or lack of appropriate digital infrastructure (30-32%), it's evident that external support is desired to be able to ease as many of these challenges as possible. This links to the feeling of unpreparedness referenced throughout sections one and two of this report, and supplier support will allow a portion of these challenges to be relieved from OEMs, freeing time and allowing more focus on designing, developing, and manufacturing the products.

Having a lack of budget being the lowest reported challenge (28%) ties to our previous sentiment that organizations are aware that putting funding towards the security of IoT and connected devices is not something that can be compromised on [page 19]. We see the same here when considering the security of manufacturing, production, or supply chain lines; budget is required for security and therefore organizations will fund it as it is critical.

Figure 11

What challenges, if any, does your organization face when considering the security of manufacturing/ production/ supply chain lines?

Respondents' organizations are OEMs of IoT/ connected devices.

Industry standards and regulation impacts

Further to the challenges experienced with the security of manufacturing and supply chain lines, almost all OEM organizations also have to navigate stringent industry standards and regulations which have a weighted impact on how they are able to move forward with the products that they design and manufacture.

Figure 12

How are industry standards, compliance requirements, and regulations impacting the manufacturing processes that produce connected/ IoT products?

Respondents' organizations are OEMs of IoT/ connected devices.

Essentially all (99%) OEM organizations report impacts to their **manufacturing processes** when conforming to industry standards, compliance requirements or regulations, with having to vet supply chain lines for security (or passing this to suppliers) the top-rated challenge. This extends to the earlier exploration of impacts on the **development** of IoT and connected devices [pages 21–22] where the sentiment and top challenge reported is relating to the supply chain and its security.

This is evidently an area where organizations are feeling pressure to get right, with the impacts of insufficient cybersecurity, or any gaps in security, a deep concern. With many of these impacted areas, organizations could seek to work with an external vendor to support and navigate these challenges presented by compliance to standards and regulations. By having a guiding hand from a vendor with expertise and experience, OEM organizations can spend more of their valuable time in designing and developing security elements for the products themselves.

The true cost of certificate management

For some organizations, a large proportion of their manufacturing lines are supported by IoT devices and connected products, so being able to maintain production without certificate outages is a necessity to prevent further cost incurrence.

However, this in itself is presenting a challenge, with 98% of organizations having experienced certificate outages in the last 12 months. The total average cost to organizations for certificate outages on their manufacturing lines in the last 12 months is staggering, at over $2,250,000. This represents a significant cost to many organizations, which will have severely impacted their ability to direct budgets towards preventing security incidents on their devices. The cost is also higher in APAC ($2,843,888) and North America ($2,610,714), demonstrating a challenge felt in these regions in particular.

The good news is that there are obvious solutions on the market, with PKI solutions prominent in assisting organizations with certificate management. A proportion of organizations are not yet using PKI (6%), and many OEMs are using internal solutions only (27%). With this being a widely outsourceable solution, it begs the question as to why more organizations aren't considering an external PKI solution to ease the concern and inevitable financial risk surrounding certificate outages.

Figure 13

For certificate outages experienced on your organization's manufacturing line, what was the total cost to your organization in the last 12 months?

Showing average cost, split by region. Respondents' organizations are OEMs of IoT/ connected devices.

Global	$2,302,278	–
APAC	$2,843,888	+$541,610 vs total
North America	$2,610,714	+$308,436 vs total
EMEA	$2,056,405	-$245,873 vs total

Lifetime responsibility of IoT and connected products

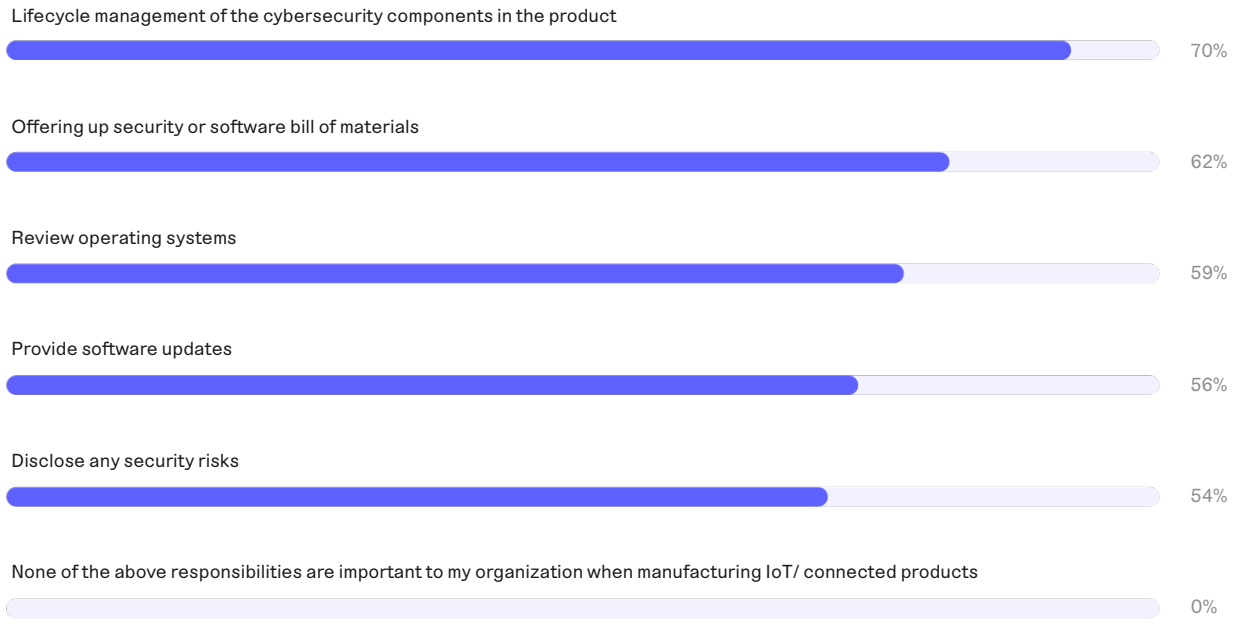
When designing and manufacturing IoT or connected products, OEM organizations recognize they have multiple areas of responsibility for security of devices across the entire lifecycle of a product.

All (100%) OEM organizations agreed that the responsibilities listed below are important to their organization when manufacturing IoT and connected products, with lifecycle management of cybersecurity components in the product being the top responsibility (70%). It's important that organizations have this level of awareness that their obligation does not end as the product is sold, and that ongoing support and development against the increasing cyber threats is vital. As we have seen, continuing to develop security for already existing devices is key for OEMs to prevent possible liability when cyber breaches occur [page 23].

Figure 14

As a manufacturer of IoT/ connected products, what are the top responsibilities to the customer that your organization has over the security of the final product?

Combination of responses ranked first to third. Respondents' organizations are OEMs of IoT/ connected devices.



However, it's not to be forgotten that keeping an open and transparent line of communication with operators and users of their products will help to ensure that the products are protected as much as possible. Over half of OEMs (54%) believe that disclosing security risks is a responsibility, however if more organizations took this approach, it would provide the potential for more collaborative work with operator and user organizations, working together to take steps to prevent any known security risks, and ultimately protect products to a greater extent. With approaching half (45%) of OEM organizations strongly agreeing that IoT security should be considered at the product design stage, it's clear that more need to demonstrate they are vigilant and proactive in the security of their devices over their entire lifecycle, from design conception to their final use.

Summary for OEM organizations

OEM organizations should consider:

- Maintaining the position of security at the heart of product design and development is vital for IoT and connected products to withstand the elevated security threats towards these devices
- Using many of the methods available to ensure the connected devices and IoT products they design and manufacture are secure
- Working with a third-party supplier to mitigate the challenges of certificate outages or production line downtime will reduce financial concerns — with PKI solutions a recognizable solution that would assist with this challenge
- Placing the product lifecycle as a top priority is key to ensure that their products will appeal to organizations that look to use and operate IoT and connected devices
- Continuing to support devices with security patches and software updates will reduce possible liability, and provide assurance that products are as protected as they can be
- Securing already deployed devices (brownfield) is a quick way to deliver heightened security to potential flaws that exist in products

Section 4

Operator and user organizations

In this section, we take a closer look at insights shared by respondents representing operator and user organizations. We have organized the topics in the following order:

1. IoT and connected product usage and investments
2. Diving into the increase in product usage
3. The risk of cyber attacks on IoT and connected devices
4. The cost of inadequate device security
5. The consequence of device attacks
6. Moving from naivety to cyber resilience

IoT and connected product usage and investments

Across many industries and sectors, organizations have embraced IoT and connected product technology, and actively operate and utilize them in their day-to-day work. Usage has developed significantly in the past few years, driven by substantial investments made by organizations to capitalize on the promise of connected devices. However, alongside this rapid expansion comes a host of security concerns that must be addressed by organizations that are falling short of adequately protecting their IoT infrastructure. Though to start with, it's important to begin by understanding what organizations have seen as the most critical elements of this technology and where they have been placing their investments.

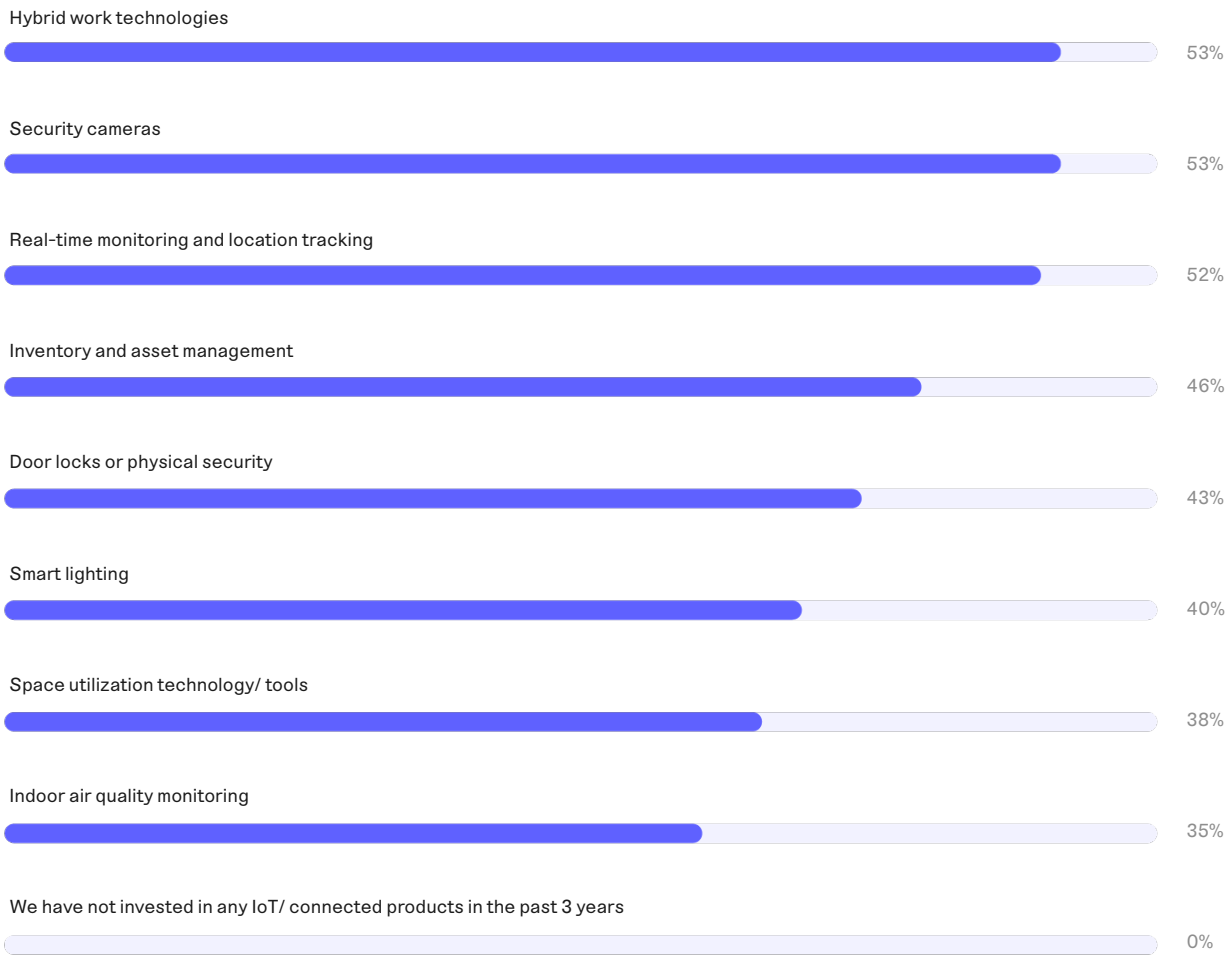
All organizations that operate and use IoT and connected devices have invested further in this area in the past three years, with hybrid working technologies, security cameras, and real time monitoring and location tracking being the top investment areas. Perhaps unsurprisingly, hybrid working continues to be an area in which organizations are seeking support from devices as changes in working patterns and location continue to be in demand following the pandemic. The use of security cameras is being driven primarily by larger organizations (with over 5,000 employees), with smaller organizations pursuing real-time monitoring and location tracking (53%) as their top investment.

With an overall increase of 20% on average for the number of IoT and connected products used by organizations in the past three years, this is a substantial area of growth, and one where organizations will be feeling a need to not get "left behind". Increasing investments in IoT and connected products that can help organizations with their daily challenges allows organizations to free their time, however, as their device usage is growing, their security needs will also be growing — increasing the need for external support.

Figure 15

In the past three years, what types of IoT/ connected products has your organization invested in?

Respondents' organizations are operators or users of IoT/ connected devices. Omitting some answer options.



Diving into the increase in product usage

It makes sense that as time goes by, organizations seek to use connected products for different reasons, especially as technological advances and changes in the products' capabilities will help to solve different challenges experienced by organizations. The 20% average increase in IoT and connected product usage is largely driven by organizations with a higher employee count, who have experienced an average increase of 26% in the number of devices in the past three years, compared to smaller organizations at 19% on average.

Similarly, the increase has also been driven in large part by safety and security concerns, alongside digital transformation and the increase in hybrid working. Perhaps it is the perception that IoT and connected devices are relatively secure, and a good way for organizations to enhance their safety and security which is why organizations are turning to them in recent years. However, this view can certainly be challenged, as we see on pages 45–46. And again, we see the impact of hybrid working causing a change in habits.

Evidently, it is of huge relevance to many organizations who are turning to devices to help with security and other concerns. As usage is growing, organizations will be keenly aware that their security needs will also grow. With larger organizations seeing this growth more so in recent years, it is an area where they are seeking support to help manage this growth.

Most organizations are looking to their budgets to help support the increased product usage, with 55% reporting an increased cybersecurity budget has been central to managing this. However, additional to this, ensuring there has been increased training and awareness for employees around cybersecurity best practices has also been pivotal (53%) alongside investing in new cybersecurity solutions (51%). Looking to ensure that employees are appropriately trained and aware of threats towards devices is a necessity when considering responsibility for cyber breaches [pages 23–24], therefore almost half of organizations that are not prioritizing this are placing their devices at risk with the potential for financial consequences [page 44].

Figure 16

Which of the following, if any, has driven your organization's use of IoT/ connected products in the workplace?

Respondents' organizations are operators or users of IoT/ connected devices. Split by organization size, omitting some answer options.

The risk of cyber attacks on IoT and connected devices

The safety and security concerns that organizations using and operating IoT products experience is valid. A difficult landscape of increased cyber attacks targeted towards IoT and connected products means that organizations have increasing concern over how to protect their devices effectively, and with a vast array of attack vectors, security needs to be all-encompassing.

69%

of organizations have seen an increase of cyber attacks on their IoT devices in the last three years

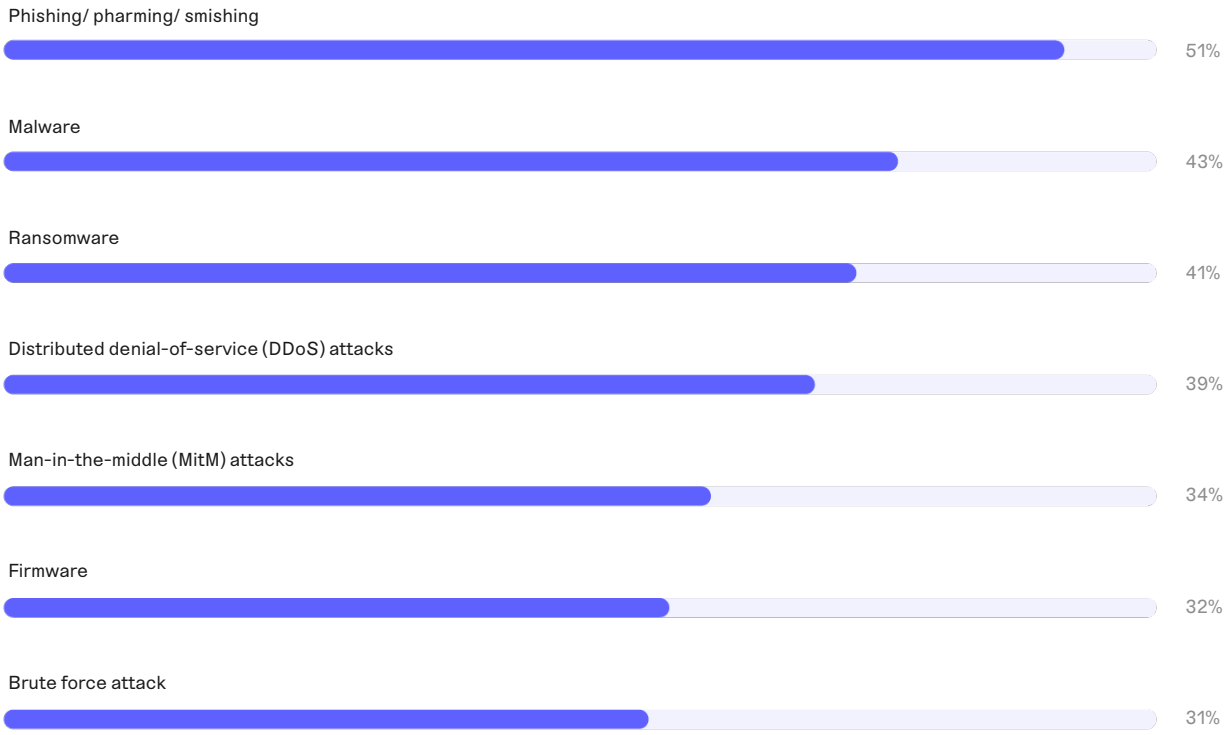
It's clear that most will not escape their devices being targeted, with cyber attacks appearing almost inevitable — almost 9 in 10 organizations have experienced attacks towards their IoT and connected devices in the past 12 months. And further to this concern, is the multiple attack vectors that these attacks are coming from; with phishing/pharming/smishing (51%), malware (43%), and ransomware (41%) the top experienced by those that have experienced a cyber attack in the past 12 months.

Therefore, it's no wonder that organizations have high concerns when it comes to device security. Over two thirds (69%) report that their IoT devices have seen an increase in cyber attacks in the last three years, and it doesn't look as though this will change going forward. Organizations therefore need to be a step ahead when thinking about their product security, ensuring that their device security covers many possible avenues of attack. Simple actions such as ensuring multi-factor authentication (MFA) is active to verify users' identities and ensuring employees are trained and aware of attack vectors are initial steps to take. With 73% of organizations agreeing that ransomware poses a considerable threat to their organization's IoT devices, ensuring that anti-malware software is up to date and monitored can help to ease this concern.

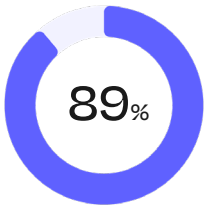
Figure 17

Of the following attack vectors, which if any, has your organization experienced in the last 12 months on IoT/ connected products?

Showing the results of those that have experienced a cyber attack in the past 12 months. Respondents' organizations are operators or users of IoT/ connected devices. Omitting some answer options.



89% of respondents said their organization's IoT/ connected products have faced cyber attacks in the last 12 months.



The cost of inadequate device security

With cyber attacks an increasing risk for IoT and connected devices [pages 42–43], the cost of cyber breaches has the potential to be substantial and very damaging for organizations looking to use IoT and connected devices to their full potential.

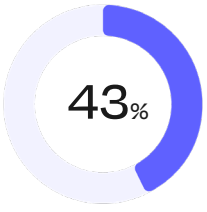
$236,035
(USD)

is the average total cost of cyber breaches experienced through organizations' IoT/ connected products in the last 12 months

Over half of organizations' annual budget for securing their IoT and connected devices is vulnerable to being diverted to cover the cost of successful breaches. On pages 19–20 we explored average annual budgets for IoT device security, and 52% of the 2023 budget could be diverted to the cost of cyber breaches on IoT and connected devices should they be successful ($236,035). This is considerable for organizations and demonstrates that the cost of cyber breaches is increasingly severe. It is leaving organizations with less than half of their original budget to spend on securing the devices in the first place, and if more than one breach is successful then organizations will struggle to place any budget in this area.

Organizations therefore need to be increasingly vigilant with their IoT and connected device security, otherwise financial consequences have the potential to be very damaging. With most believing that users of IoT and connected devices have an element of responsibility alongside the organizations that manufacture these devices, organizations need to take responsibility in ensuring that their device security is up to date, and that those that use these devices are aware and compliant when it comes to avoiding falling victim to any attacks. Implementing training, clear processes, and procedures will ensure compliance and reduce liability should any cyber attacks be successful.

43% of the cyber attacks experienced in the last 12 months were on IoT/ connected products, on average



The consequence of device attacks

As well as fearing the financial cost of cyber attacks, organizations also have other concerns should an unsecured IoT or connected product result in a cybersecurity intrusion. External reputation damage, losing customer data, and losing employee data are the top concerns, however it is interesting to consider the top impacts by those that **have** experienced cyber attacks on their IoT or connected devices in the past 12 months, compared to those that **have not**.

For organizations that have experienced cyber attacks, they are more likely to report concerns in all areas, with relatively high scoring across the board. Comparing this to those that **have not** experienced attacks, the concern varies in different areas, with higher concern for losing customer data and low concern for employees losing confidence. It indicates that there is a preparedness that comes with experience of having experienced a cyber attack. These organizations understand that **all** the areas are important and can be of consequence, and this is a learning for organizations yet to experience an attack on their IoT devices. Being prepared in a multi-faceted way is essential to avoid the potential consequences of a cyber attack.

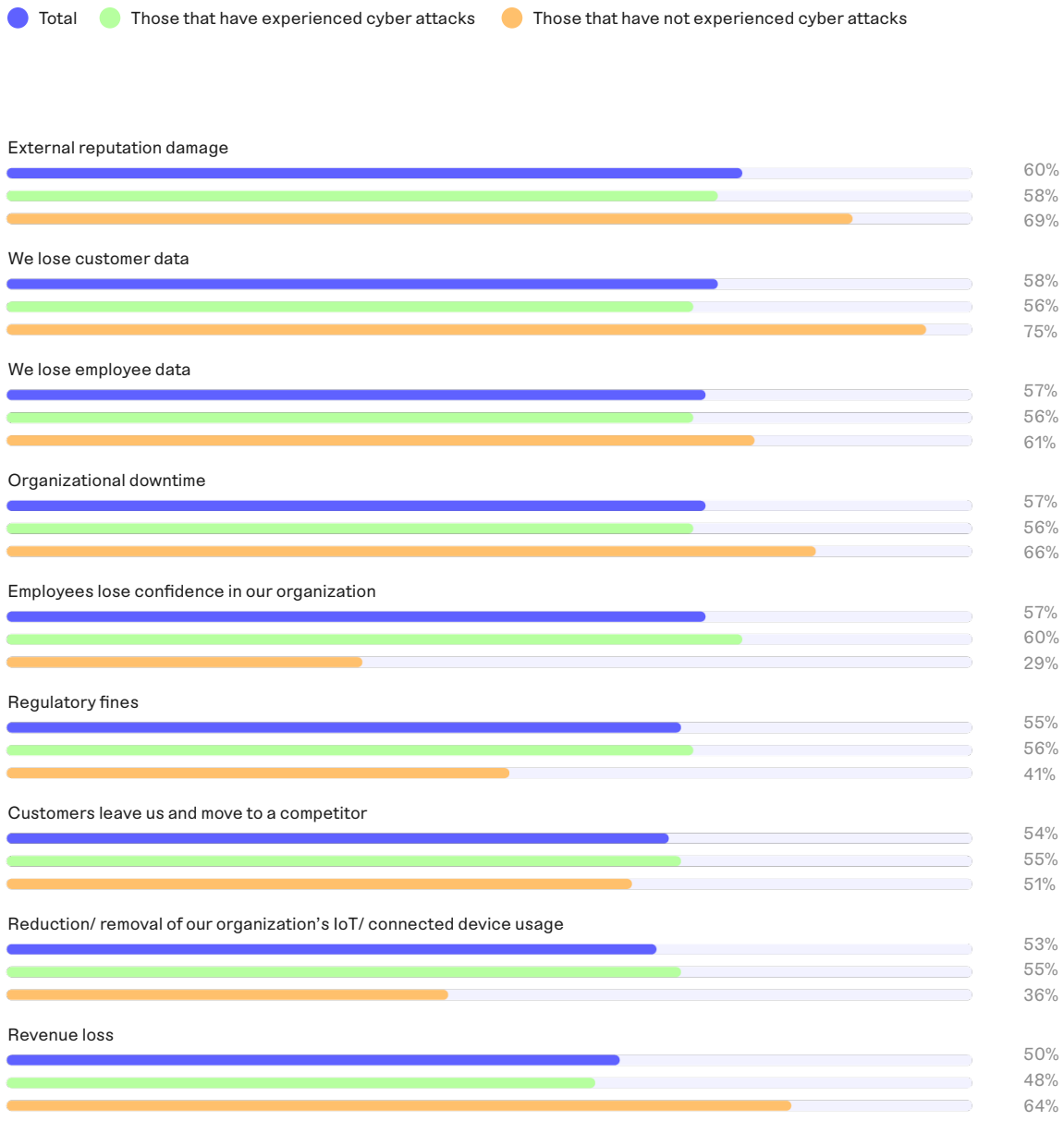
Further to this, seeing that revenue loss is reported as the least concerning impact, this suggests a level of naivety for many organizations. It could be that there is not a full understanding of the financial impact of a cyber breach and the consequences that it could have. It could be that there is not a full understanding of the financial impact of a cyber breach and the consequences that it could have.

This ties to some areas that we have already explored, with organizations considering themselves “fully” protected against attacks [pages 10–11]. Organizations may consider themselves fully protected, as they have considered the attack avenues and consequences that they may experience should a cyber breach occur. However, if an element hasn’t been fully protected, or an attack avenue not fully explored, perhaps the consequence of not protecting this isn’t fully realized. Organizations can take the experiences of those that have faced attacks and ensure that all consequences are considered and prepared for, to lessen the impacts should a cyber breach be successful.

Figure 18

If your organization were to experience a cybersecurity intrusion resulting from an unsecured IoT/ connected product, what impact most concerns you?

Combination of responses ranked first to fifth. Respondents' organizations are operators or users of IoT/ connected devices. Split by those that have or have not experienced cyber attacks in the past 12 months, omitting some answer options.



Moving from naivety to cyber resilience

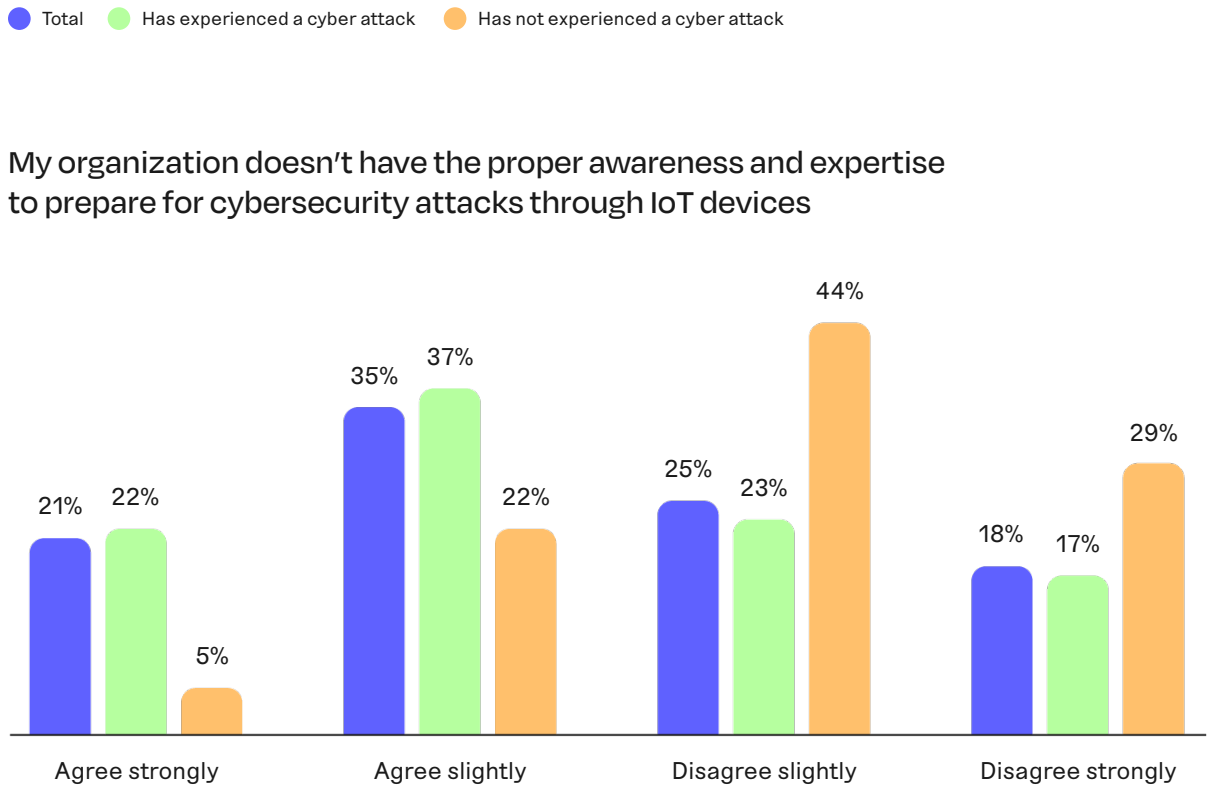
With it being increasingly evident that organizations that operate and use IoT and connected devices are struggling under the weight of increased devices, increased targeted attacks towards these devices, and the consequences following, it's clear that there is a need for improvement.

Over half (56%) agree that their organization doesn't have the proper awareness and expertise to prepare for cybersecurity attacks through IoT devices, with 1 in 5 (21%) strongly agreeing to this.

Figure 19

To what extent do you agree or disagree with the following statements?

Respondents' organizations are operators or users of IoT/ connected devices. Showing split of those that have/ have not experienced a cyber attack in the past 12 months. Omitting some answer options.



Furthermore, the view that organizations that have not experienced cyber attacks have a level of naivety regarding attacks is compounded with almost three quarters reporting a disagreement with the statement that they don't have proper awareness and expertise to prepare for cybersecurity attacks on their devices (73%). With these organizations feeling they have awareness and have the ability to deal with attacks, it is clear that they aren't considering the far-reaching effects that other organizations are considering. For those that have experienced attacks, more respondents strongly agree that they do not have full awareness and expertise to prepare for attacks compared to those that have not experienced attacks, suggesting they are more realistic and aware of the ever-changing nature of attacks and the ways in which they can infiltrate IoT and connected devices.

Perhaps some organizations are resigned to the fact that an increase in devices comes with additional threat and associated impacts, however many do recognize that support can provide relief. Many report that introducing a PKI solution to issue digital identities on IoT and IIoT devices will provide them with benefits (87%), and also utilizing a certificate lifecycle automation platform to manage certificates (89%) is seen as a realistic solution. Reviewing the suitability of these solutions for organizations could help to provide a key advantage when trying to get ahead of cyber threats and manage the security of their devices.

Summary for operator/ user organizations

Operator/ user organizations should consider:

- How their product usage has changed in the past year, and the reasons for these changes — would they benefit from support in managing the security of additional devices
- Possible attack vectors, and how cyber-criminals are attempting to attack their devices. Do they have full protection across all possible avenues?
- Ensuring that their employees are appropriately aware of attack vectors, and the proper processes and procedures to follow when using devices to ensure their security
- The impacts of incomplete security on their devices; from financial consequences to reputational damage, to losing data, and beyond
- Placing a focus on all impacts of a successful cyber breach, ensuring that all areas are considered and prepared for
- Taking the experiences and lessons learned from organizations that have experienced successful cyber breaches in recent years. How theses breaches occurred, and the impacts experienced can help organizations be vigilant — with this knowledge they can prepare for and prevent future attacks

Conclusion

Organizations are battling an increasingly threatening world when it comes to protecting their IoT and connected products. They know they need to secure their devices, but a level of complacency is concerning; organizations believe that they are protected, without **fully** considering if they are.

With the security of IoT devices being of prominent importance, organizations cannot afford to **not** adequately protect their devices, whether they design, manufacture, operate, or use them. The significant costs to annual security budgets for IoT and connected products are at risk of being diverted to the cost of successful cyber breaches, or to the cost of certificate outages on manufacturing or production lines. Organizations cannot be complacent in allowing these to occur, as it takes from the initial budget to protect the devices in the first place — causing a potential cyclical effect whereby attacks happen as budget hasn't been forthcoming. With the liability for cyber breaches thought to be equal responsibility for users and manufactures of devices, security must be prioritized at both ends. Ensuring that product security is managed throughout its lifecycle is necessary to prevent the risk of new threats from the varying attack vectors.

A marked area in which organizations can further improve their device security is through third-party vendor support, which is sought after by many organizations. Having additional support to face the challenges they are experiencing could be crucial for organizations that are struggling with the increased threat of cyber attacks. PKI solutions to manage certificates and digital identities, or certificate lifecycle automation platforms are recognizable sources of support and can undoubtedly eliminate costly certificate outages. However, seeking support with vendors brings a new set of challenges. Finding a trusted supplier who will provide transparency and clarity will establish a thriving working relationship and ease many of the challenges that organizations are currently juggling.

Additional resources

eBook: Eight Steps to IoT Security

Implementing cybersecurity for IoT devices doesn't have to be complex. Discover an eight-step framework to help you plan for security at the onset of your next project.

Learn more ↗

White paper: Five Guiding Tenets of IoT Security

Learn why the potential of IoT security hinges on our ability to build a solid foundation across the IoT ecosystem, consisting of devices built with security and the necessary properties to ensure it endures.

Learn more ↗

Keyfactor for Smart Home: Making Matter-compliant devices with security by design

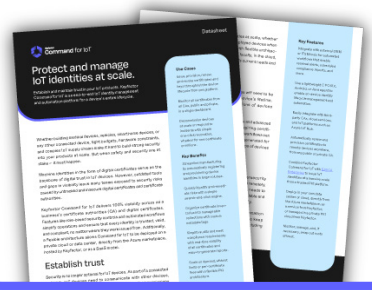
Discover how to establish trust and compliance in Smart Home and consumer IoT devices with identity-first security.

Learn more ↗

Keyfactor Command for IoT: Protect and manage IoT identities at scale

Find out how to create and maintain trust in your IoT products by protecting and managing their identities at scale.

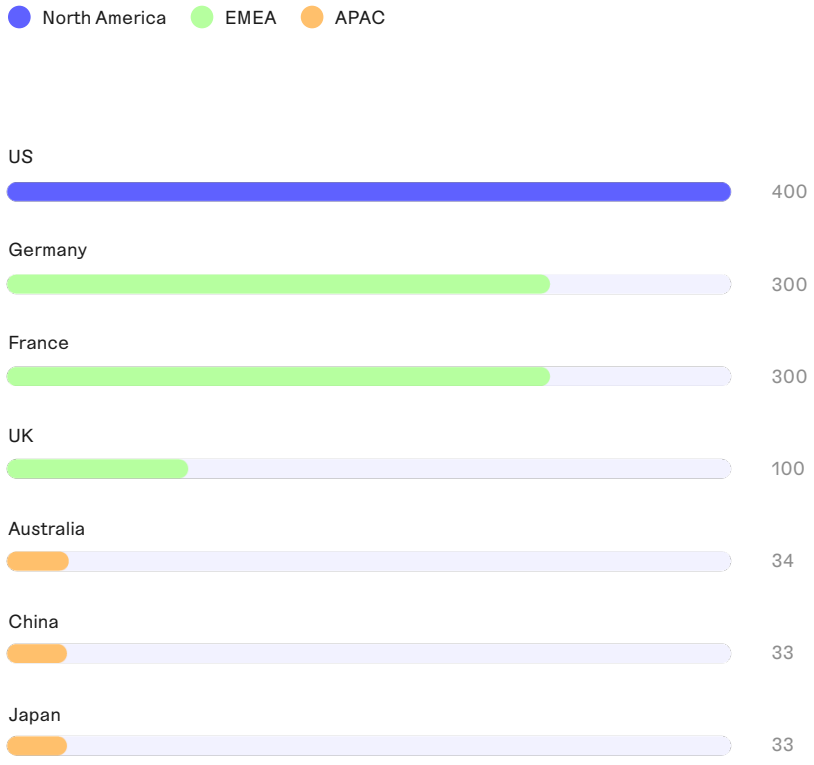
Learn more ↗



Research methodology

Keyfactor commissioned independent market research agency Vanson Bourne to conduct research into the state of IoT security.

The study surveyed 1,200 IoT and connected product professionals in June and July 2023, all of whom had some responsibility or knowledge of IoT or connected products within their organization. Respondents were from the US, UK, Germany, France, Australia, China, and Japan.



1,200

IoT and connected product professionals surveyed

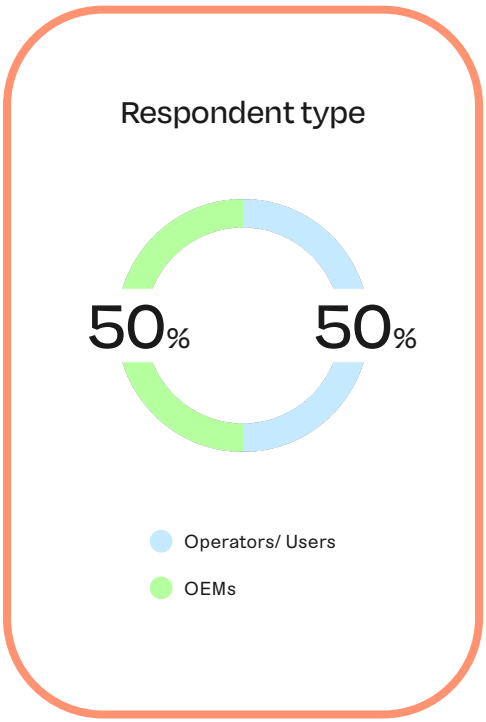
Respondents were from organizations with 500 to 5,000 or more employees, across the following sectors: manufacturing and production, IT, technology & telecoms, energy, oil/ gas & utilities, retail, distribution & transport, media, leisure & entertainment, construction & real estate/ property, financial services, business & professional services, consumer services, and the public sector.

Respondents were from organizations who were either manufacturers (OEMs) of IoT and connected products, or were operators or users of IoT and connected products.

- OEM organizations were from the manufacturing sector, who were involved in designing IoT or connected products, manufacturing them, or both
- Operator/user organizations were from any sector (including manufacturing), who operate or use connected products in their factory, facility, or enterprise (no involvement in design or manufacture)

All respondents had an element of knowledge or responsibility for IoT or connected products in their organization, including setting the strategy or being involved in strategic decision making.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.



About Keyfactor and Vanson Bourne

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter, and advocate of growing a trusted, secure, diverse, and inclusive workplace.

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.