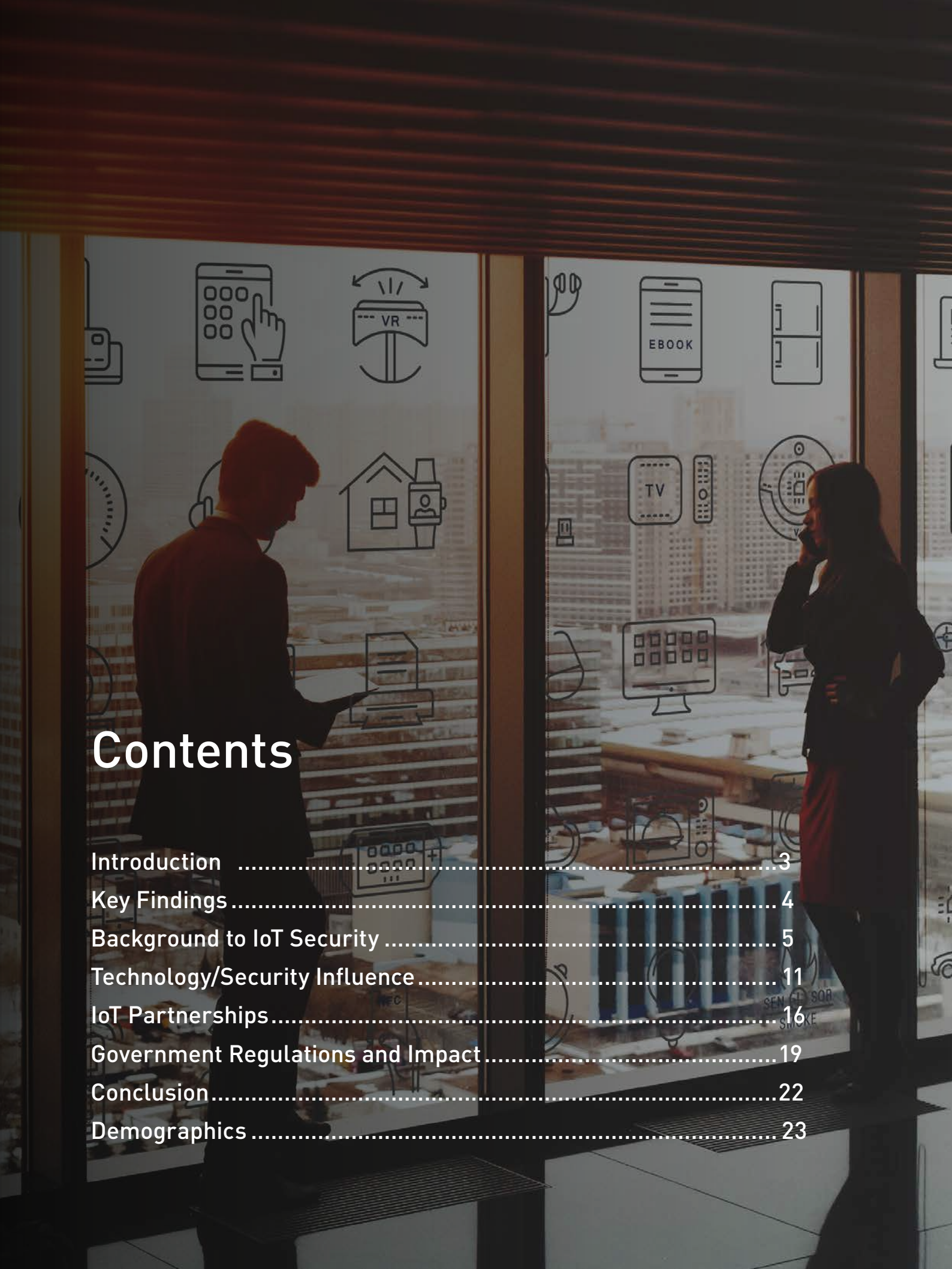
THE STATE OF IOT SECURITY

gemalto
security to be free

IoT device breaches undetectable by nearly half of companies

Use of blockchain technology to help secure IoT data, devices and services doubles in a year



Contents

Introduction

Almost half of companies still can't detect if any of their IoT devices has been breached. Use of blockchain technology to help secure IoT data, devices and services doubles in a year

With the number of connected IoT devices set to top 20 billion by 2023, businesses must act quickly to ensure their IoT breach detection is as effective as possible.

Surveying 950 IT and business decision makers globally, Gemalto found that companies are calling on governments to intervene, with nearly four in five (79%) asking for more robust guidelines on IoT security, and more than half (59%) seeking clarification on who is responsible for protecting IoT. In fact, most (95%) businesses believe there should be regulations in place, a finding that is echoed by consumers, nearly all (95%) of which expect IoT devices to be governed by security regulations.

Almost half, 48%, of businesses aren't able to detect if any of their IoT devices suffers a breach. This comes despite companies increasing focus on IoT security:

- Spending on protection has grown (from 11% of IoT budget in 2017 to 13% now);
- Nearly all (90%) believing it is a big consideration for customers when using IoT products; and
- Almost three times as many now see IoT security as an ethical responsibility (14%), compared to a year ago (4%).

Given the increase in the number of IoT-enabled devices, it's extremely worrying to see that businesses still can't detect if they have been breached. With no consistent regulation guiding the industry, it's no surprise the threats – and, in turn, vulnerability of businesses – are increasing. This will only continue unless governments step in now to help industry avoid losing control.

Security remains a big challenge

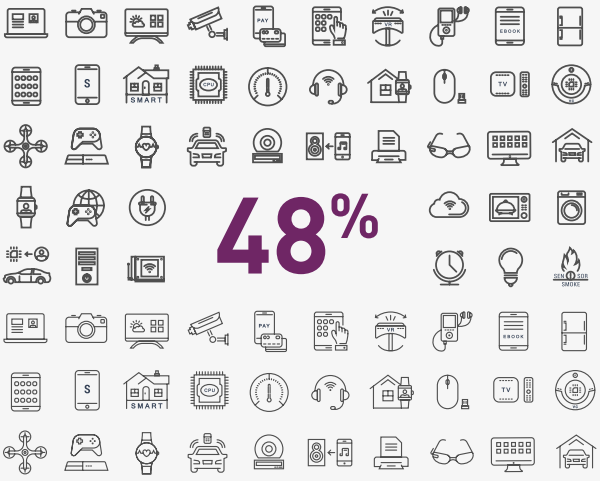
With such a big task in hand, businesses are calling for government intervention because of the challenges they see to securing IoT devices and services, notably data privacy (38%) and collecting large amounts of data (34%). Protecting an increasing amount of data is proving an issue, with only three in five (59%) of those using IoT and spending on IoT security, admitting they encrypt all of their data.

Consumers1 are clearly not impressed with the efforts of the IoT industry, with 62% believing security needs to improve. In fact, when it comes to concerns regarding IoT, over half (54%) fear a lack of privacy because of connected devices, followed closely by unauthorised parties like hackers controlling devices (51%) and lack of control over personal data (50%).

Blockchain gains pace as an IoT security tool

While the industry awaits regulation, it is seeking ways to solve the issues itself, with blockchain emerging as a potential aid; adoption of the technology has doubled from one in 10 (9%) to a fifth (19%) in the last 12 months. What's more, a quarter (23%) of respondents believe that blockchain technology would be an ideal solution to use for securing IoT devices, with nine in 10 (91%) organisations that don't currently deploy the technology likely to consider it in the future.
As blockchain technology finds its place in securing IoT devices, businesses continue to employ other methods to protect themselves against cybercriminals. The majority (71%) encrypt their data, while password protection (66%) and two factor authentication (38%) remain prominent. Most are also aware that they need to do better, with over half (54%) of IoT device manufacturers and IoT software service providers increasing their IoT security offerings for customers over the last year and nearly three fifths (57%) adopting a security by design approach.

Key findings



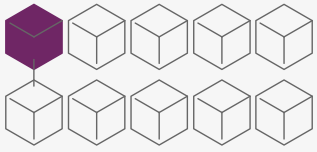
of companies can detect if their IoT devices suffers a breach

48%

of companies believe security is a big consideration for customers with 14% seeing it as an ethical responsibility

79%

of companies call on governments globally to provide more robust guidelines on IoT security

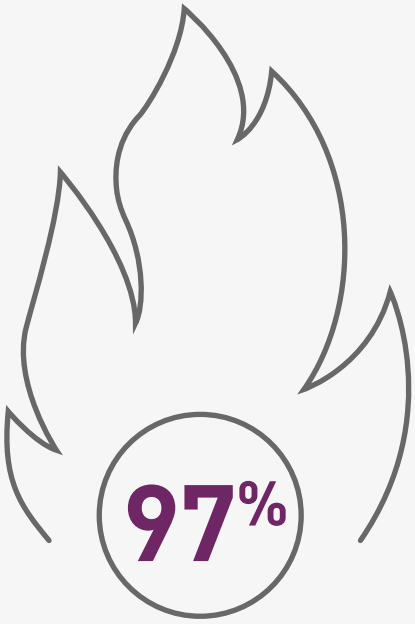


10%

of companies increase of use of blockchain technology to help secure IoT data, services and devices (up from 9% to 19%)

59%

of companies encrypt all their IoT related data



of companies see a strong approach to IoT security as a key competitive differentiator

54%

of manufacturers or service providers increased their IoT security offerings for customers over the last year

Background to IoT security

IoT involvement

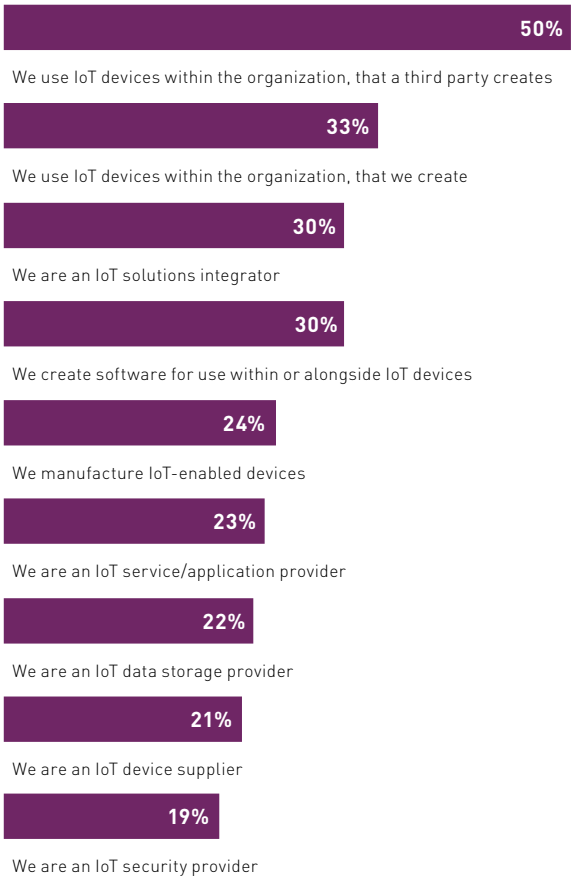
Half (50%) of those surveyed say that their organization uses IoT devices that a third party creates

A third (33%) report that their organization uses IoT devices that they create, while three in ten are an IoT solutions integrator (30%) and/or create software for use within or alongside IoT devices (30%)

A multitude of organizations exist within the IoT ecosystem, making the connections between them both important and potentially complex

> Are organizations doing anything differently due to the rise in IoT devices?

What involvement does your organization have with IoT?



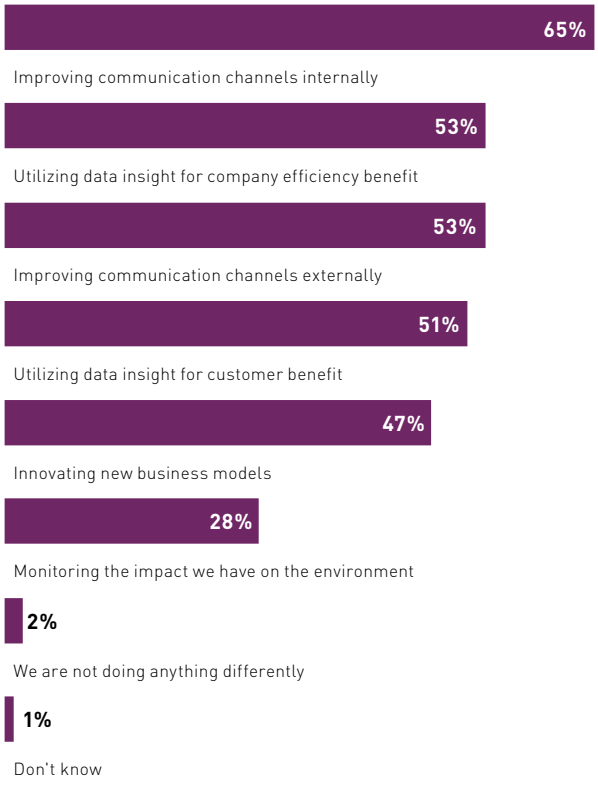
Changes due to IoT

IOT USERS

Of respondents whose organizations are using IoT devices, almost all (96%) state that their organization is doing something differently as a result of more devices becoming IoT enabled

Improving communication channels internally (65%) and externally (53%) are some of the most likely changes, while 53% are utilising data insight for efficiency benefits, which suggests that positive impacts have been felt

As an IoT user, is your organization doing anything differently as a result of more devices becoming IoT enabled?



IOT ENABLERS

The vast majority (98%) of respondents whose organizations provides IoT manufacturing, software, services, applications or security, say that their organization is doing something differently as a result of more devices becoming IoT enabled

Increasing product/service range (55%) and IoT security offerings (54%) are the most likely changes, suggesting that new products could have security as a key component

As an IoT enabler, is your organization doing anything differently as a result of more devices becoming IoT enabled?

Spending on IoT security

On average, 13% of respondents' organizations' IoT spend is on the security of their products or services, which is slightly higher than it was in 2017 (11%). Of those whose organization stores data or uses IoT devices and invests in their IoT security, fewer than three in five (59%) encrypt all of the data that they capture or store via IoT devices, with this being lowest in the UK (53%) and Japan (50%)

Spend on IoT security appears to have risen slightly, yet many organizations are still not encrypting all of their data, which could mean that they are prioritizing their security spend in other areas

---

Analysis of the average percentage of respondents' organizations' IoT spend that is on the security of their IoT products or services, showing 2017 and 2018 data

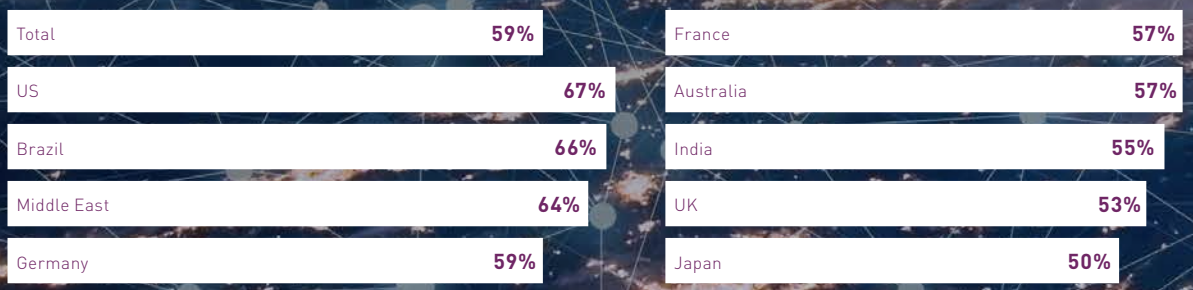
2017 AVERAGE IOT SPEND ON SECURITY

11.07%

2018 AVERAGE IOT SPEND ON SECURITY

13.15%

Fig 7
Analysis of respondents' organizations who encrypt all of the data that they capture or store via IoT devices, split by respondent country



Encryption of IoT data

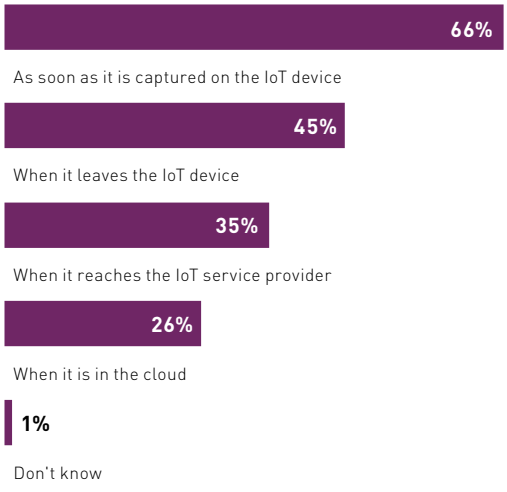
Of respondents whose organizations encrypt at least some of the data that it captures or stores via IoT devices, two thirds (66%) report that their organization encrypts IoT data as soon as it is captured

Of those whose organization stores data or uses IoT devices, spends on the security of their IoT products/ services and encrypts at least some of the data it captures or stores via IoT devices, a slightly lower (59%) proportion state that this is the case when they send data via IoT devices

Anyone who is not encrypting their IoT data as soon as it is captured/sent could be leaving their data in a vulnerable position

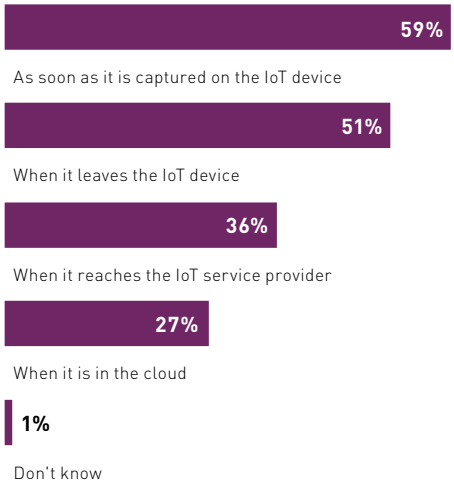
ENCRYPTING CAPTURED/STORED IOT DATA

At what points is the data that your organization captures/stores via IoT encrypted?



ENCRYPTING SENT IOT DATA

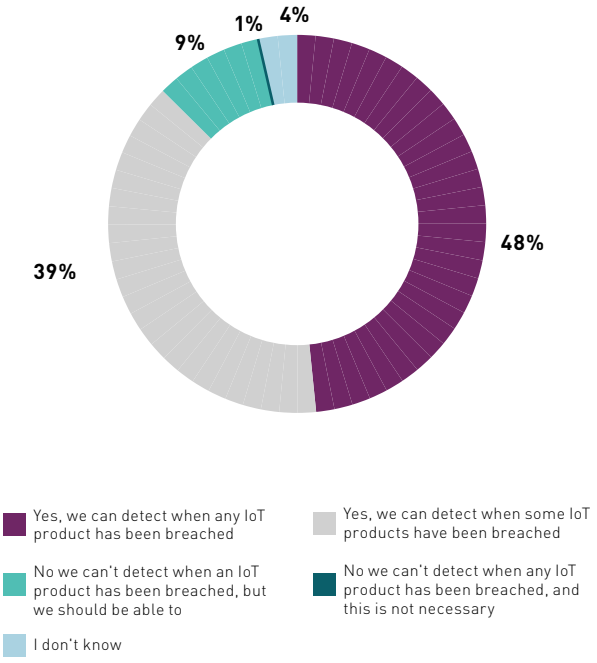
At what points is the data encrypted that your organization sends via its IoT devices (e.g. communications between devices)?



Detecting a breach on IoT devices

Almost nine in ten (87%) respondents' organizations can detect when at least some of their IoT products have been breached, but only 48% can detect when this happens to any IoT product. How does this vary by country?

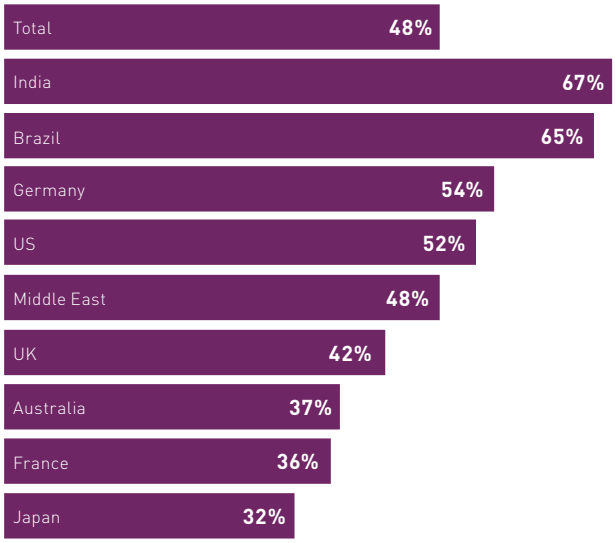
Can your organization detect when an IoT device has been breached?



Respondents in India (67%) and Brazil (65%) are the most likely to report that their organization can detect when any of their IoT products have been breached, with this being far less likely (32%) for those in Japan (who are also the least likely to encrypt all their data at)

If organizations cannot detect when a product is breached, then a hacker could be inside their system for a much longer period of time

Analysis of respondents' organizations that can detect when any of their IoT products have been breached, split by respondent country



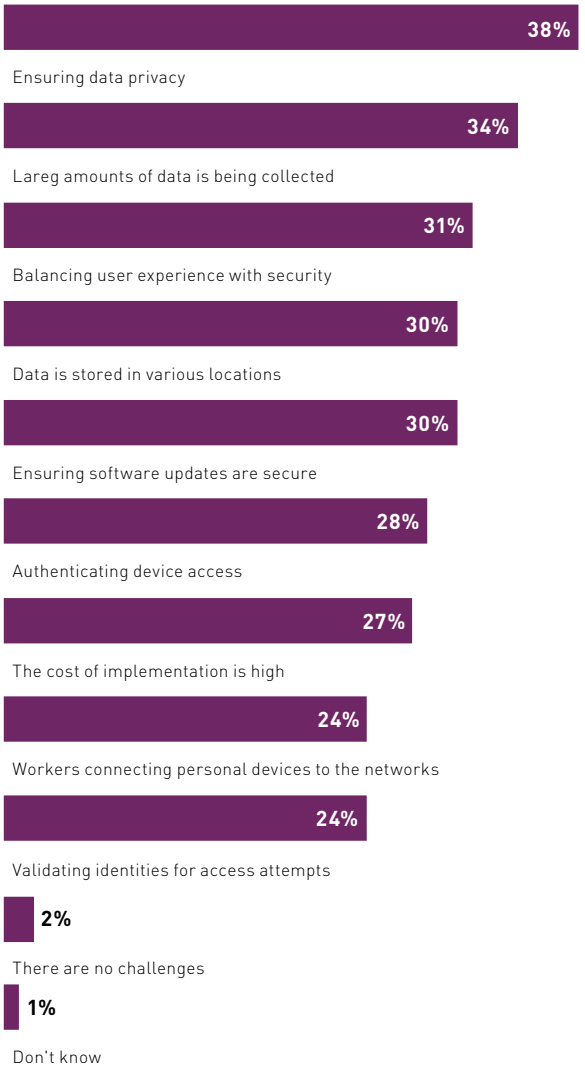
Challenges when securing IoT products

The most likely challenges are ensuring data privacy (38%) and large amounts of data being collected (34%)

Furthermore, around three in ten say that balancing user experience with security (31%) and/or that ensuring software updates are secure (30%) are challenges

The proportion of organizations seeing security challenges shows how difficult of an area this is and suggests that organizations might need to increase their use of encryption more quickly and to a greater scale than they are currently doing

What challenges does your organization see with trying to secure IoT products/ services?



Technology/security influence

Describing IoT security

In 2018, 24% of respondents report that their organization sees IoT security as a secure foundation to offer new services, compared to 32% in 2017

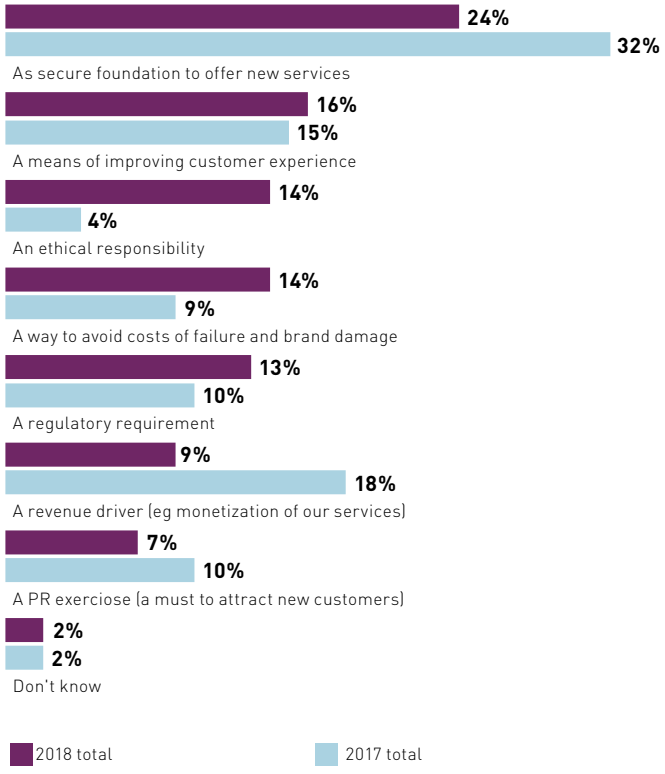
Over one in ten (14%) say that it is an ethical responsibility in 2018, which is far higher (4%) than in 2017

Fewer report IoT security to be a revenue driver in 2018 (9%) than they did in 2017 (18%)

There appears to be a shift in the reasons for deploying IoT security, but whatever they may be, IoT security is still critical in the success of an IoT platform

> Do organizations consider security when they are designing IoT products and/or offerings?

Which of the following best describes how your organization sees IoT security?, showing 2017 and 2018 data



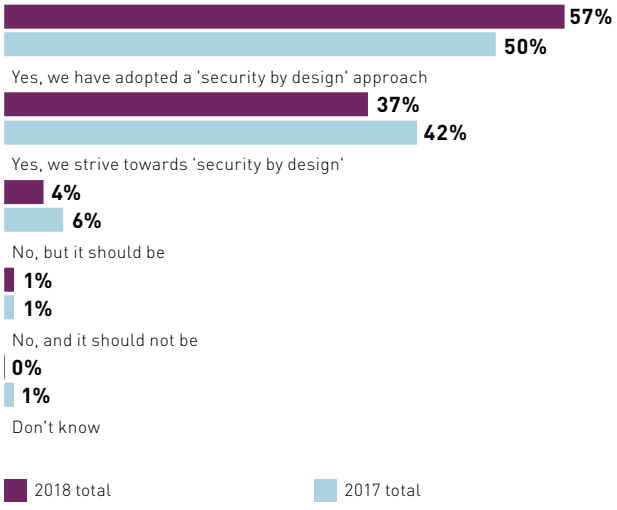
IoT security by design

Almost three in five (57%) 2018 respondents say that their organization has adopted a 'security by design' approach.

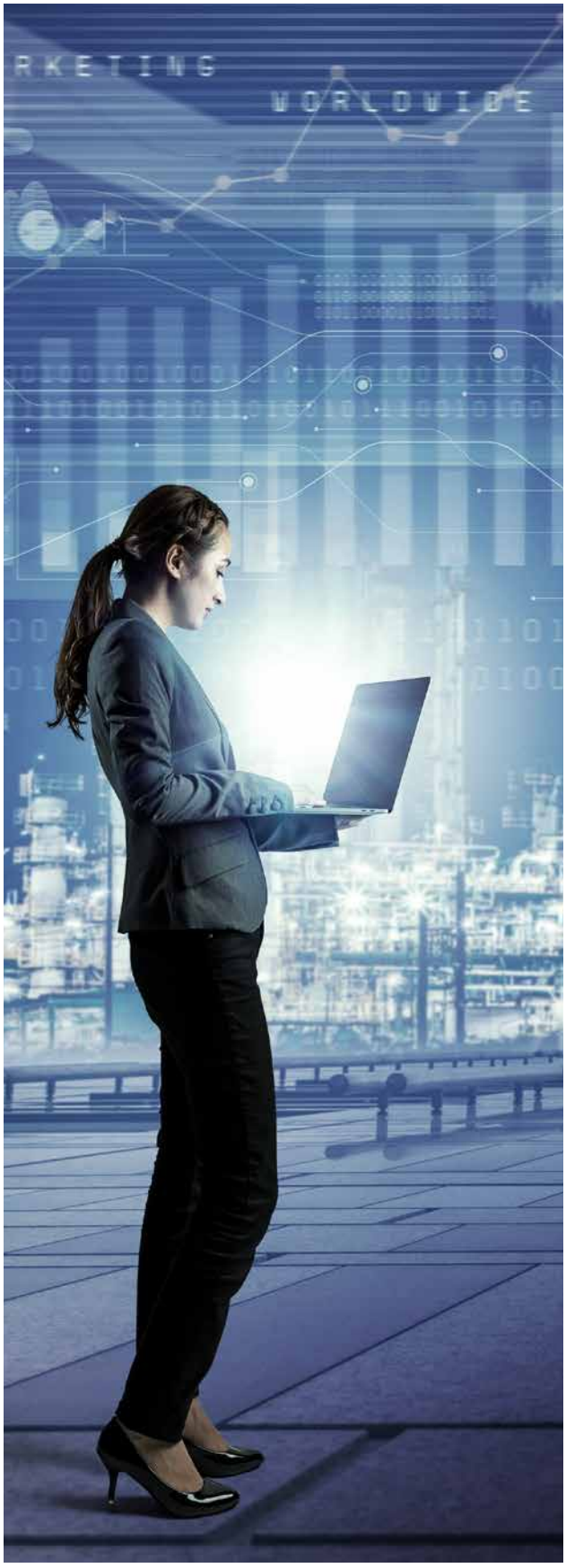
When asked to those whose organization is an IoT device manufacturer, or provides IoT software, services, applications or security

In 2017, it was only half (50%) who reported that this was the case. Organizations seem to be moving in the right direction when it comes to security by design, but many may still have challenges to overcome

Is security a consideration when your organization designs its IoT product/ offering?", showing 2017 and 2018 data



Asked to respondents whose organization is an IoT device manufacturer, or provides IoT software, services, applications or security (574 respondents in 2018 and 600 respondents in 2017)



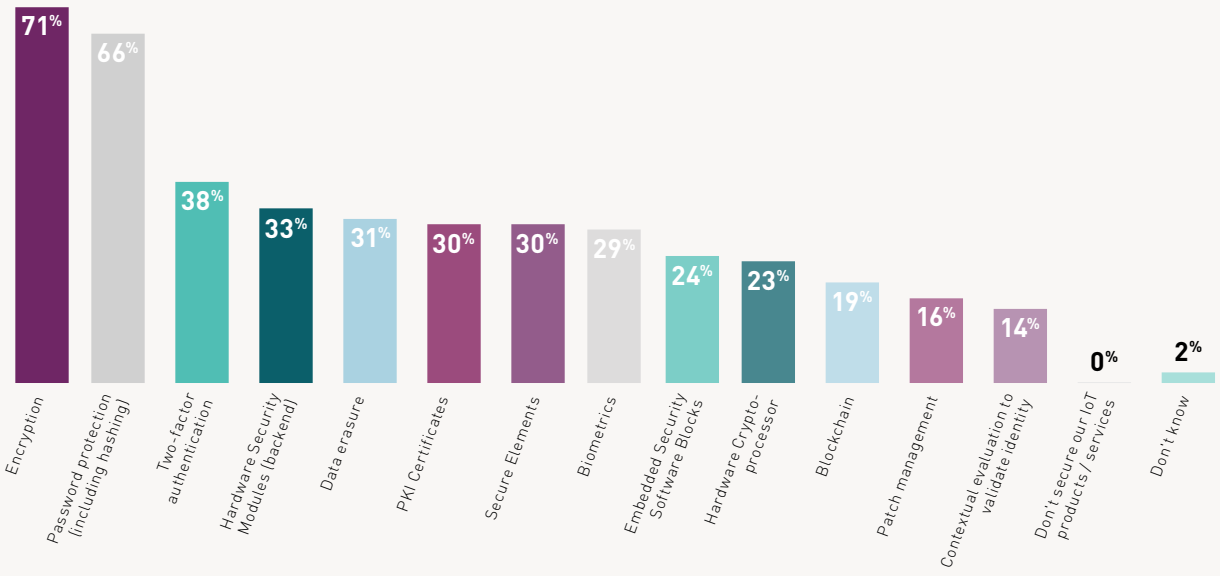
IoT security technologies

Around two thirds or more respondents state that their organization uses encryption (71%) and/or password protection (66%) to secure its IoT, with these technologies being the most likely (60% and 56%) ideal solutions

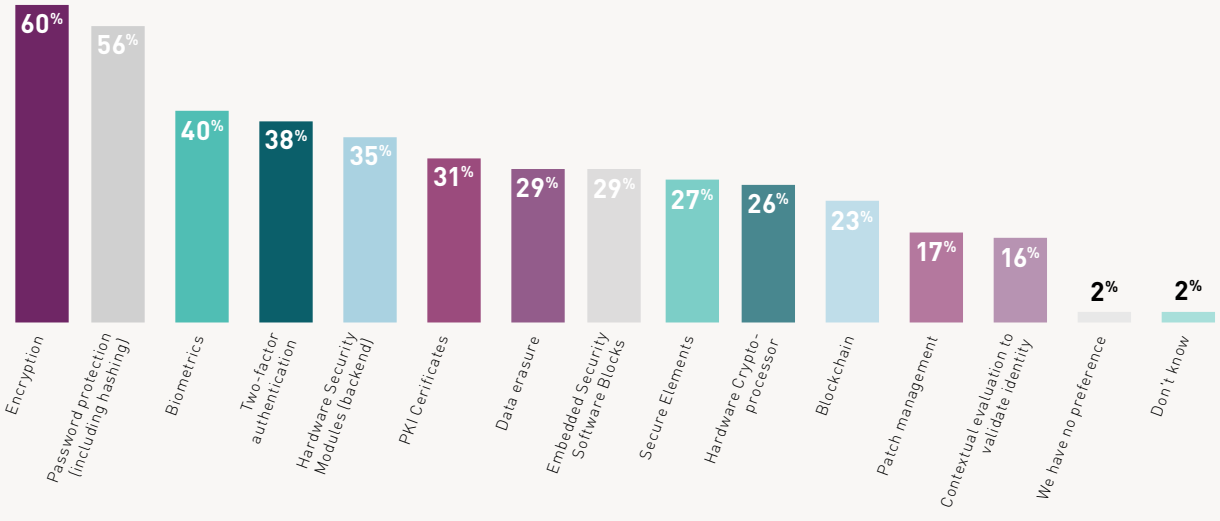
Only 19% currently use blockchain , but in an ideal world 23% would

Around three in ten (29%) use biometrics, but four in ten (40%) would like to , which suggests that some technologies are not quite as attainable as organizations would like, making the next few years extremely interesting

Which technologies does your organization currently use to secure its IoT data/services/devices?



Which technologies would your organization ideally use to secure its IoT data/services/devices?



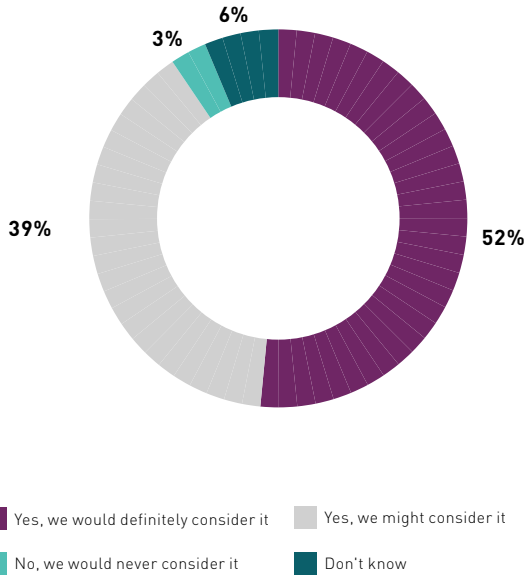
Consideration of blockchain

Of those who do not already, around nine in ten (91%) respondents' organizations would consider using blockchain in the future, but only 52% would definitely consider it

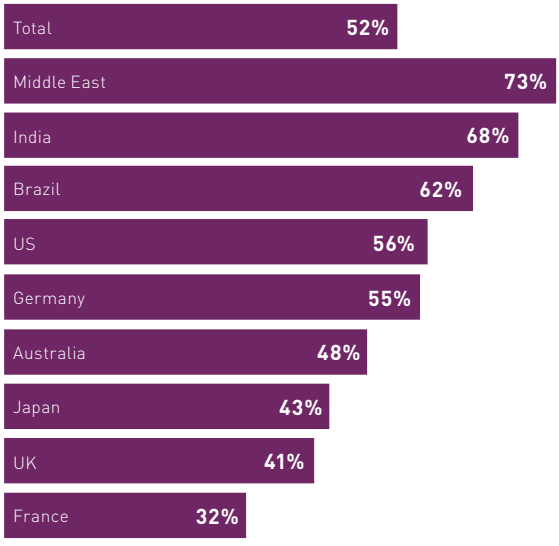
Those in the Middle East (73%) and India (68%) are far more likely to definitely consider blockchain, with those in France the least likely (32%)

With a significant proportion not yet adopting, or considering blockchain, organizations could be putting themselves at substantial risk and opening themselves up to breaches

Would your organization consider using blockchain in the future?



Analysis of respondents' organizations who would definitely consider using blockchain in the future, split by respondent country



Asked to respondents from organizations that do not use blockchain to secure its IoT data/services/devices (774 respondents)

Customers' view on IoT security

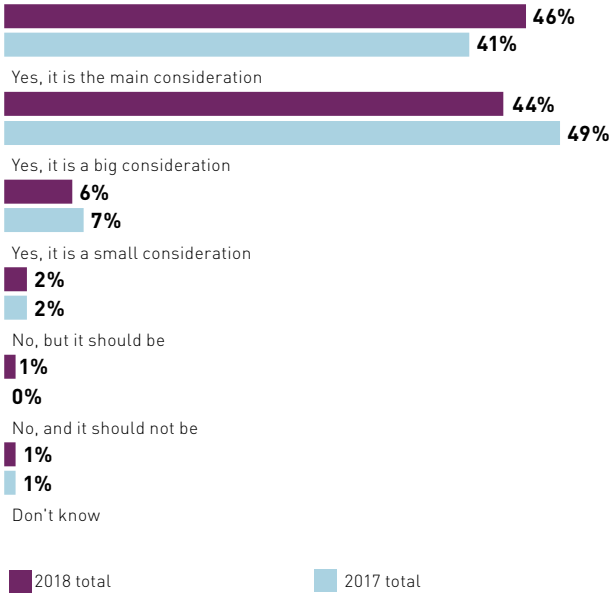
In 2018, 46% of respondents state that security is the main consideration for customers when using IoT products/offerings

This was slightly lower (41%) in 2017, which suggests a marginal shift in the importance of IoT security to customers and organizations should change their priorities accordingly

Organizations are now more likely to take a 'security by design' approach, but many could still be doing more than they currently are to meet these customer considerations

> Do respondents see IoT security as a competitive differentiator?

Do you think security is a consideration for your customers when they are using your IoT products/offerings?



Asked to respondents whose organization is an IoT device manufacturer, or provides IoT software, services, applications or security (574 respondents in 2018 and 600 respondents in 2017)

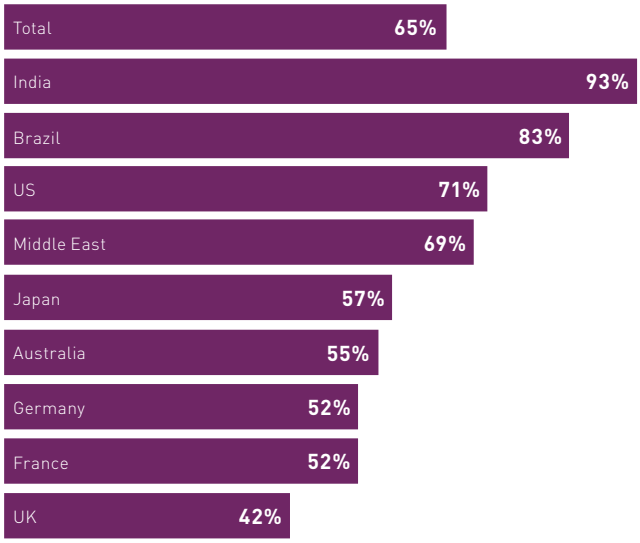
Security as a differentiator

Almost two thirds (65%) of those surveyed cite that a strong IoT security approach is definitely a competitive differentiator when asked to those whose organization is an IoT device manufacturer, or provides IoT software, services, applications or security

This is far higher (93%) in India, but is much lower (42%) in the UK

Customers tend to consider IoT security when using IoT products/offerings, which reinforces that security can be a differentiator and the need to have a 'security by design' approach

Analysis of respondents who definitely see a strong IoT security approach as a competitive differentiator, split by respondent country



Asked to respondents whose organization is an IoT device manufacturer, or provides IoT software, services, applications or security (574 respondents)

IoT partnerships

IoT partnerships

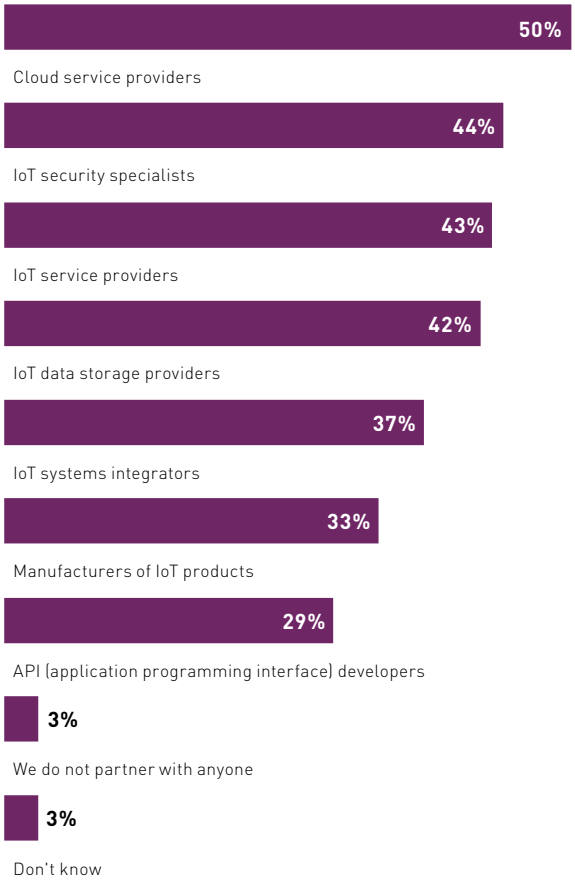
Over nine in ten (95%) respondents' organizations partner with another organization when it comes to IoT Cloud service providers (50%) are the most likely source of partnership

What are the reasons for partnering with other organizations?

Keeping data secure when it is in the cloud (41%), first collected (40%) and when applying software updates (39%) are the most likely reasons for partnering with other organizations in relation to IoT

Security appears to be the most likely driver for partnerships, which could help to drive security as a differentiator

Who does your organization partner with regarding IoT?



Why do you choose to partner with other organizations in relation to IoT?

Asked to respondents whose organization partners with other organizations regarding IoT (899 respondents)

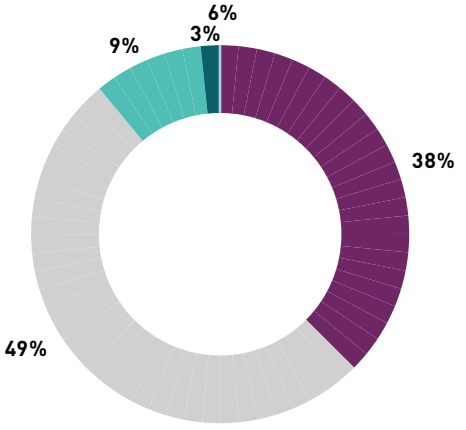
Working with an IoT partner

Of respondents whose organization uses IoT and partners with other organizations, almost all (96%) report that they have some control over data as it moves from partner to partner, but only 38% say that they have complete control

Improvements to IoT partnerships could be made through a better use of security technology (58%), more transparency over data security (53%) and/or better guidance from IoT security experts (53%)

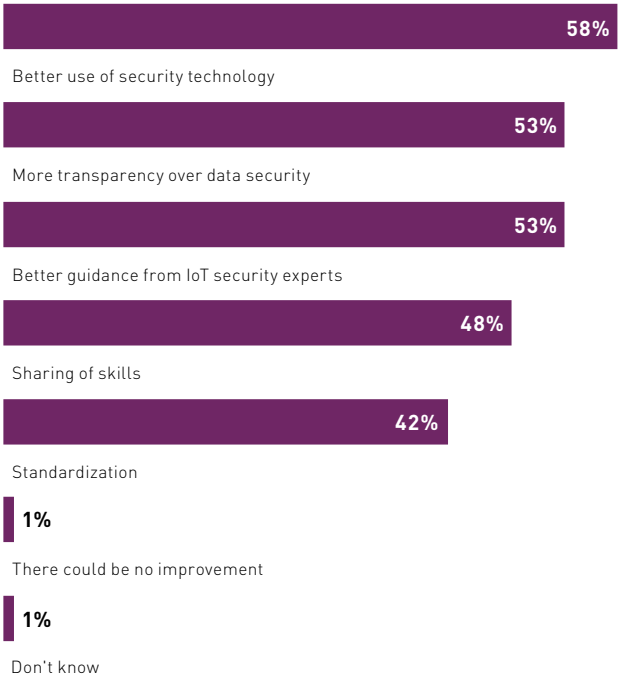
While partnerships are in use and can provide a range of benefits they are still not perfect and organizations could benefit even more if they improve those partnerships

Do you have control over the data your IoT products/services collect as it moves from partner to partner?



Asked to respondents whose organization uses IoT and partners with other organizations regarding IoT (568 respondents)

Which of the following could help your organization improve the way it partners with other organizations in relation to IoT?



Asked to respondents whose organization partners with other organizations regarding IoT (899 respondents)

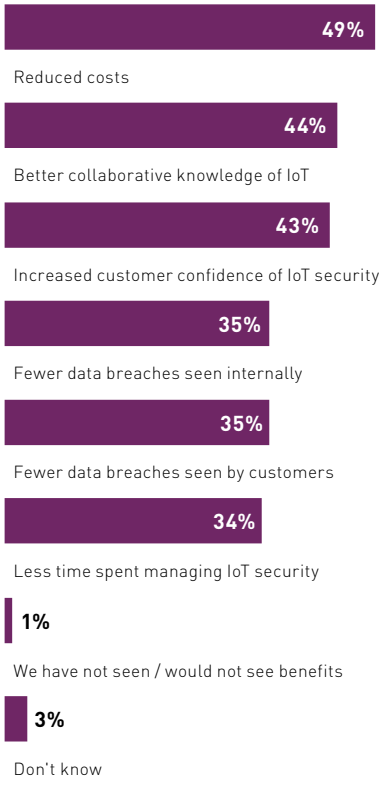
IoT security benefits of partnering

Nearly all (96%) respondents say that their organization has/would see benefits through partnering with other organizations in relation to IoT security

The most likely benefits are reduced costs (49%), better collaborative knowledge of IoT (44%) and increased customer confidence of IoT security (43%)

Security is a key reason for partnering with other organizations and there can be benefits tied in, but organizations should still keep greater visibility and control over their data

What benefits have/would your organization see as a result of partnering with other organizations in relation to IoT security?



Government regulations and impact

IoT security regulations

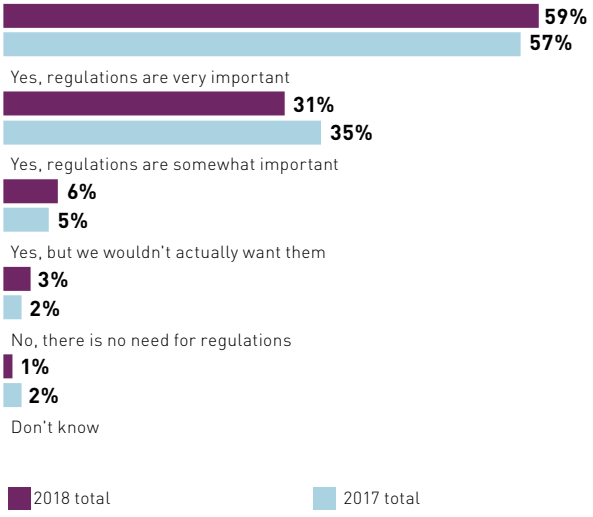
Over nine in ten (95%) respondents state that there should be IoT security regulations

Almost six in ten (59%) state that these regulations are very important, which is a slight increase (57%) from 2017

Security is becoming even more pivotal in IoT and regulations would help to ensure that all organizations are keeping their (and their customers') data safe

> What should be included within IoT security regulations?

Do you think there should be regulations in place regarding IoT security?, showing 2017 and 2018 data



IoT security regulations inclusions

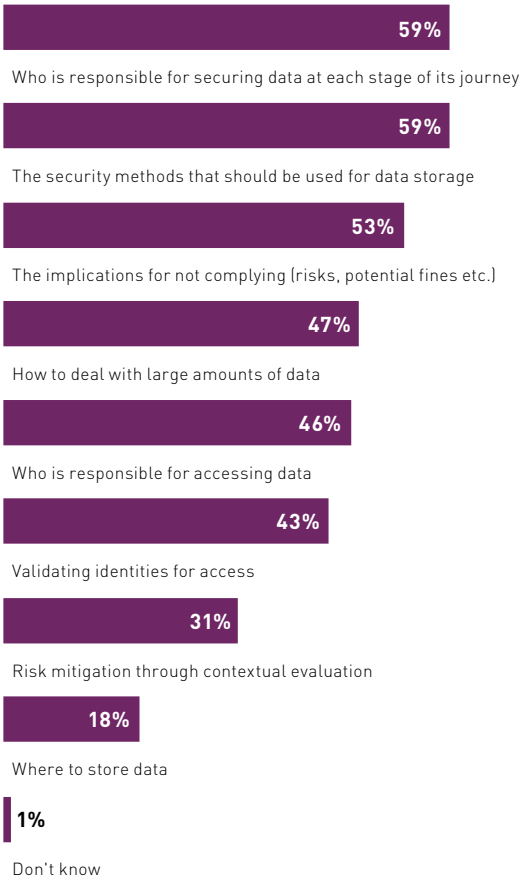
Of respondents who feel that there should be IoT security regulations, 59% state that they should include who is responsible for securing data

The same proportion (59%) state that the security methods that should be used for data storage should be a regulation inclusion

Fewer than one in five (18%) state that where data is stored should be included. However, this should be considered as a key component to ensuring that data is visible and secure, particularly as many organizations do not have complete control over IoT data as it moves from partner to partner

> Who should be responsible for abiding by IoT security regulations?

What should be included within IoT security regulations?



Asked to respondents who think that there should be IoT security regulations (907 respondents)

Abiding by IoT security regulations

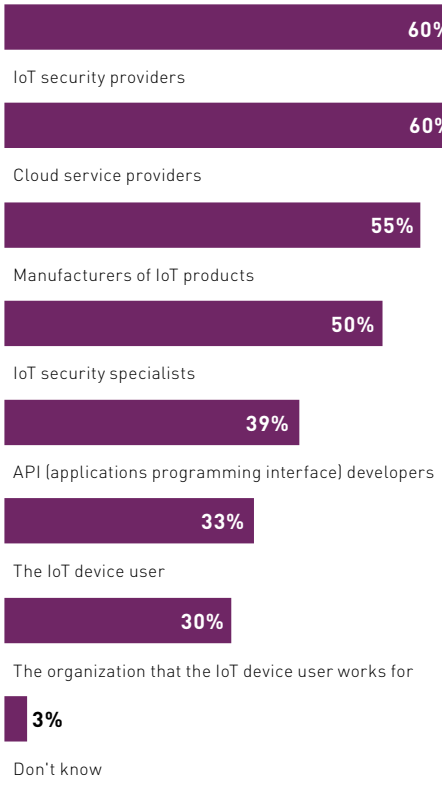
Six in ten respondents feel that IoT (60%) and/or cloud (60%) service providers should abide by IoT security regulations

Half or more say the same when it comes to manufacturers of IoT products (55%) and/or IoT security specialists (50%)

The best case scenario is that everyone abides by IoT security regulations, and doing so in partnerships in order to minimize the risk of a breach

> Are there any other concerns that respondents have surrounding IoT?

Who should be responsible for abiding by IoT security regulations?



Asked to respondents who think that there should be IoT security regulations (907 respondents)

Concerns over IoT

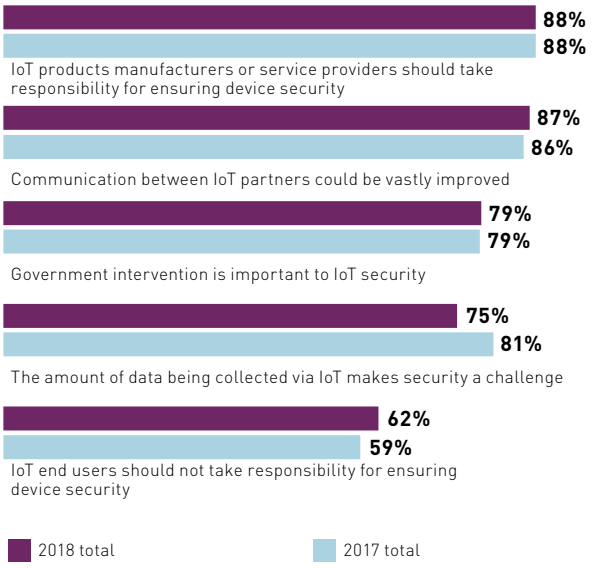
Almost nine in ten (87%) agree that communication between IoT partners could be vastly improved

Just under four in five (79%) state that government intervention is important to IoT security

These percentages remain comparable to 2017, which suggests that these challenges and opinions are not going away and could continue in the future

IoT can bring about vast benefits, but organizations need to ensure that they keep their security investment up, because if they do, it can be the differentiator between themselves and their competitors

Analysis of respondents who agree with the below statements, showing 2017 and 2018 data



Conclusion

Many organizations are embracing the Internet of Things (IoT) as part of their digital transformation. In so doing, enterprises are connecting a growing number and variety of IoT devices to their corporate networks. These devices interact with other valuable IT assets and sometimes handle sensitive information. It's therefore important that companies take steps to secure their IoT devices.

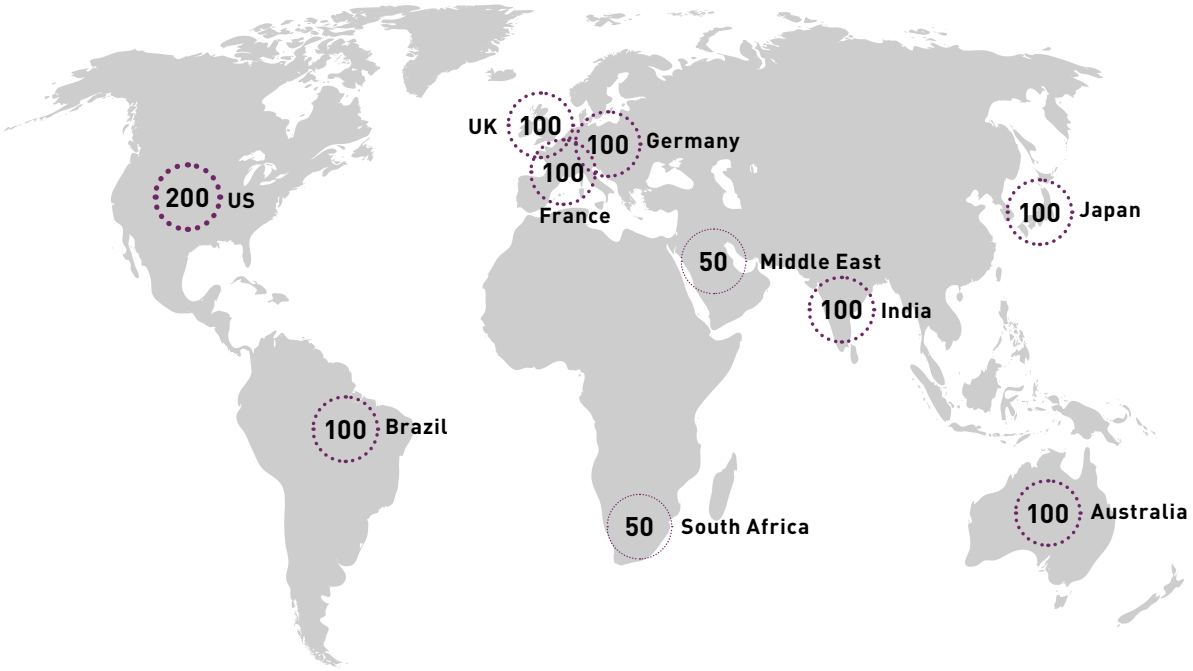
Unfortunately, IoT security isn't as easy as it sounds. More numerous and varied smart devices create a multifaceted IoT ecosystem, which adds to the complexity of the IT environment in general. Such intricacy creates digital risk, as attackers have a greater number of devices to target and asset relationships to abuse. Additionally, smart products don't handle data the same way or send information to the same location. Some devices may take less precautions than others, thereby jeopardizing organizations' data security.

Businesses are clearly feeling the pressure of protecting the growing amount of data they collect and store. But while it's positive they are attempting to address that by investing in more security, such as blockchain, they need direct guidance to ensure they're not leaving themselves exposed. In order to get this, businesses need to be putting more pressure on the government to act, as it is them that will be hit if they suffer a breach.

IT Decision makers (ITDM) demographics

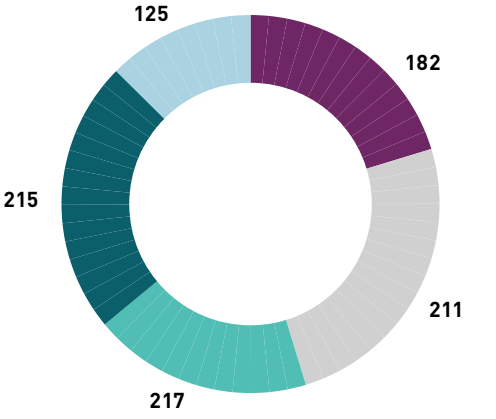
950 IT and business decision makers with awareness of IoT in their organization were interviewed in May and June 2018, split in the following ways

Country



Analysis showing respondent country (950 respondents)

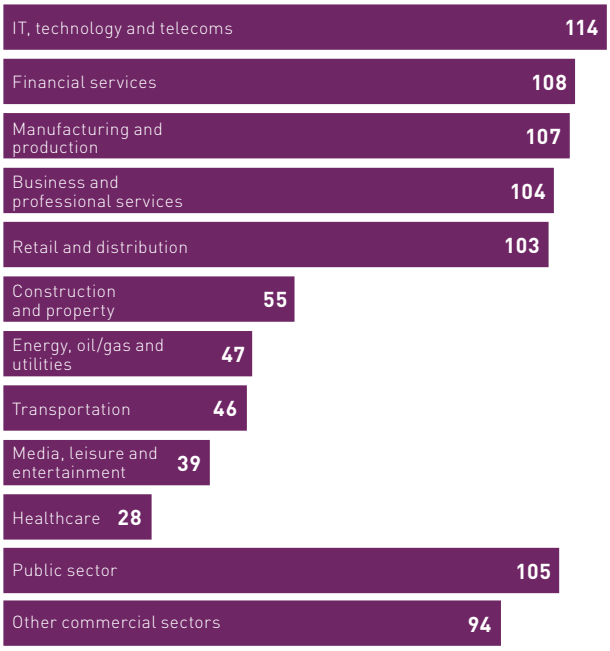
Organizational size



- 251-500 employees
- 501-1000 employees
- 1001-3000 employees
- 3001-5000 employees
- More than 5000 employees

Asked to all respondents (950 respondents)

Organization sector



Asked to all respondents (950 respondents)

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For more Gemalto research, visit safenet.gemalto.com/data-security-trends
Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free