# THE STATE OF IoT SECURITY

## Security takes a back seat

Is it time for government-mandated IoT security regulations?


Powered by gemalto

# Is it time for government-mandated IoT regulations?

The rise of IoT is driving increasing concern about the threat of cyber attacks at home and work. This trend has sparked a security concern across the globe with companies and consumers as smart devices like baby monitors, smart speakers, smart watches or thermostats potentially provide a gateway into users' home or workplace networks.

The pace of change and technological advancements are increasing. More and more organizations are connecting through IoT and monetizing IoT can be a key factor between a business being successful and being left behind. It's also bigger than ever for consumers. A whole host of devices are being IoT enabled, from cars to kettles and lights to locks – you name it, it's becoming IoT ready. As a result, consumers have more to consider when purchasing household items and security can often be the deciding factor.

However, it's no secret that there can be challenges in securing IoT devices. More devices being IoT enabled means a more complex IoT ecosystem. In addition, more data is being collected than ever before and this data is being stored in various places, but with no clear regulation or direction on how this should work. This means that the IoT journey is not always

an easy one - but it could be. This is the right time for intervention. If governments can set regulations then faith can be restored and built into the security of the IoT ecosystem. After all, which other revolutionary technologies are left unregulated? In addition, organizations need to invest in IoT partnerships, particularly with security in mind. Consumer confidence is likely to define an organization's success in the IoT world, with security playing a huge part in that.

Now is the time for organizations and regulatory bodies to act. Many organizations are already utilizing IoT, but with a lack of clear direction. If organizations do not secure their devices, their competitors will. Those who do not risk losing their competitive advantage, customers and financial gains. Ultimately, it could see them becoming a dinosaur in a digital age, ceasing to exist.

### Scope of research (methodology)

Gemalto commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this whitepaper is based.

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

**This research identifies the following:**

- The current state of the IoT ecosystem
- How technology and security influence IoT
- The partnerships forged between organizations
- Whether there should be IoT government regulations
- Consumers' perception of IoT

A total of 1,050 IT and business decision makers and 10,500 consumers were interviewed in July 2017, via online and telephone methodology. Decision maker respondents were from organizations in any sector, but with a minimum of 250 employees. Respondents were from within the following countries:

## Countries surveyed

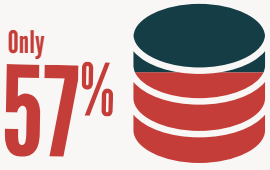

IoT Devices - Please consider IoT devices throughout this report as any internet-connected object able to collect and exchange data, and that can be monitored and/or controlled from a remote location. Examples of IoT devices include smart watches (e.g. Apple Watch, Fitbit, etc.), in-house heating systems (e.g. Hive etc.), smart speakers (e.g. Amazon Echo, Google Home), security systems (e.g. IP camera, connected alarm panel etc.), home comforts (e.g. smart lighting, smart garden irrigation, etc.), connected cars, drones etc.

# Key findings


96% of businesses and 90% of consumers believe there should be IoT security regulation


of consumers own an average of four IoT devices, but only 14% believe that they are knowledgeable on IoT device security


of consumers are concerned about a hacker controlling their IoT device while 60% are concerned about data being leaked




of businesses encrypt all of the data that they capture or store via IoT devices


of businesses feel IoT regulations should include who is responsible for securing data at each stage of the journey


of businesses believe they have complete control over the data that their IoT products/ services collects as it moves from partner to partner, potentially leaving data unprotected at some stages of its journey

# Background to IoT

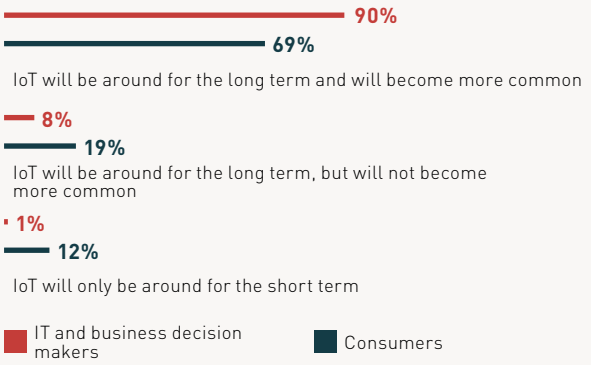
The internet of things (IoT) is here. IoT is a technology trend that is gaining in profile and credibility and with that comes a vastly complex IoT ecosystem. Just over half (51%) of surveyed IT and business decision makers report that their organization uses IoT devices that have been created by a third party. Around three in ten use IoT devices that they create themselves (30%) or create software for use within or alongside IoT devices (28%). More and more organizations are connecting with IoT in an attempt to steal a competitive advantage and prevent themselves falling behind. Organizations can now work alongside one another in many different ways, making for an extremely unique and diverse ecosystem.

But, it is not too late for organizations to connect with the IoT world. Nine in ten (90%) decision makers think that IoT will be around for the long term and that it will become even more common in the future. This feeling is slightly less evident (69%) among consumer respondents. The difference in opinion could be due to a lack of awareness and exposure that consumers have had with IoT. Decision makers are more likely to have had the opportunity to monetize IoT in the workplace and see the benefits that can be reaped.

With the increase in complexity and size of the IoT ecosystem, it is perhaps no surprise to see that the vast majority (94%) of decision makers, whose organization uses IoT, state that their organization is doing something differently as a result of more devices becoming IoT enabled. The most likely changes are to improve communication channels internally (58%) and externally (49%), suggesting that communication can be improved through the use of these devices. In addition, most (98%) IoT enablers are also making changes. Increasing their IoT security offering is the most common (57%) change, highlighting the importance of security within the IoT ecosystem.

**The longetivity of IoT**

"Which of the following best describes your opinion of IoT?"




Split by respondent type, asked to all respondents (1,050 decision maker respondents and 10,500 consumer respondents)

# Introducing IoT security

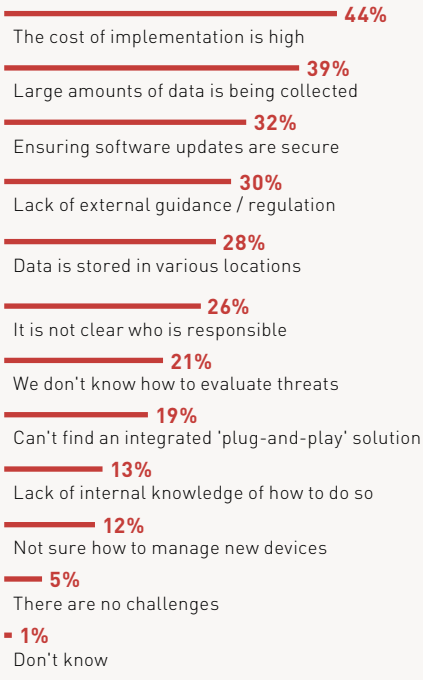
Effective IoT platforms need to be built on a secure foundation. On average, 11% of decision makers' organizations' IoT spend is on the security of their IoT products or services. But, of those who are spending on IoT security, fewer than three in five (57%) decision makers report that their organization encrypts all of their IoT data. This is just not good enough. Organizations should be utilizing encryption to provide persistent protection of IoT data at all critical points of the IoT ecosystem.

IoT security is often deemed as complicated and insufficient. More than nine in ten decision makers (94%) and consumers with IoT knowledge (93%) feel that there are challenges when trying to secure IoT products/ services. Decision makers most commonly cite the cost of implementation (44%) and large amounts of data being collected (39%) as challenges, while consumers frequently state that the lack of external guidance (43%) and a lack of clarity over who is responsible (41%) are challenges. If organizations are to successfully monetize their IoT offering then they will need to work alongside consumers to ensure that they feel comfortable and confident in the security of their devices, while harnessing data effectively, and absorbing huge financial cost. No small ask.

Additionally, over four in five (84%) consumers agree that the amount of data being collected via IoT makes privacy a challenge and a similar proportion (81%) of decision makers say the same for security. With more organizations connecting to the IoT environment and the ecosystem becoming ever more complex, these challenges are only going to increase in stature. Organizations need to ensure that they have the right resources, security systems, and knowledge and guidance in place to be successful in this digital era.

**Challenges according to decision makers**

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




Asked to all decision maker respondents (1,050 respondents)

**Challenges according to consumers**

"What challenges do you think are present when trying to secure IoT products/ services?"


Asked to consumer respondents who have some IoT security knowledge (6,729 respondents)

# Security preferences

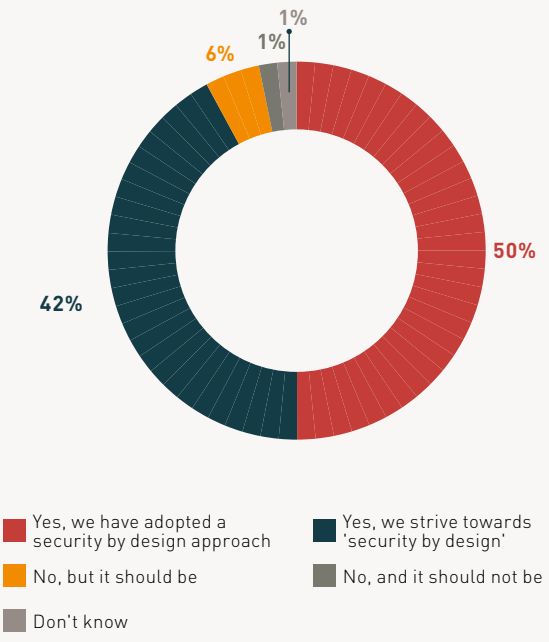
Given the challenges that IoT security can introduce, perception of IoT security is likely to vary and is often negative. But, IoT security does also have positive impacts on organizations. A significant minority of decision makers believe that IoT security is a secure foundation to offer new services (32%), a revenue driver (18%) or a means of improving customer experience (15%). Organizations must be able to see a long term goal that can be achieved through a secure IoT platform. A partnership alongside an IoT security specialist then becomes an obvious port of call.

However, IoT security is not engrained into organizations as well as it should be, yet. Only half (50%) of decision makers whose organization provides IoT manufacturing, software or services report that their organization has already adopted a 'security by design' approach, while around four in ten (42%) say that they do strive towards it. If organizations are going to overcome security challenges and fears, then adopting security as an organizational strategy and approach is likely to be crucial. This could define their ability to monetize IoT products and services.

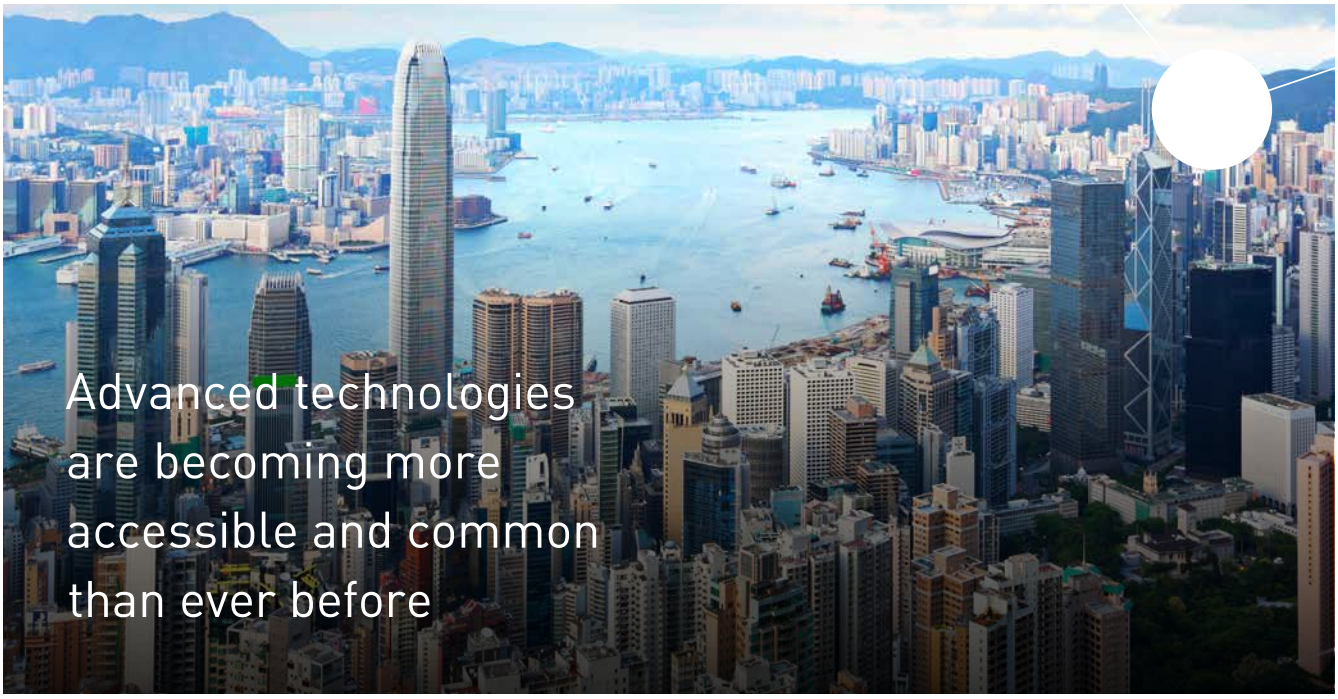
> Organizations must be able to see a long term goal that can be achieved through a secure IoT platform.

**Security by design**

"Is security a consideration when your organization designs its IoT product/ offering?"




Asked to decision maker respondents whose organization provides IoT manufacturing, software or services (600 respondents)

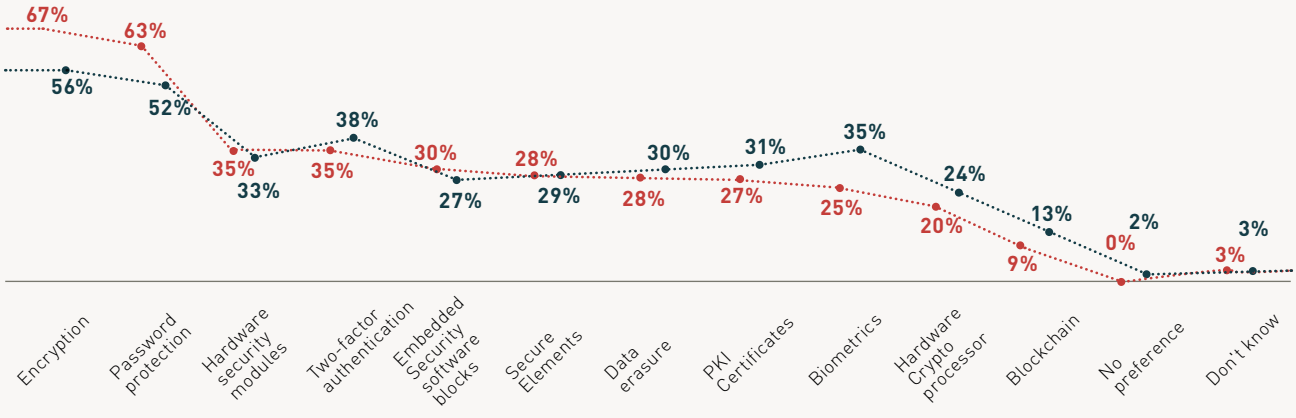


# Advanced technologies are becoming more accessible and common than ever before

The use of tools and technologies are fundamental to a secure IoT platform. Encryption (67%) and password protection (63%) are the most commonly used IoT security technologies in decision makers' organizations currently and are also seen as being the ideal ones (encryption (56%), password protection (52%). There is also a significant proportion of respondents who believe that two-factor authentication (38%) and biometrics (35%) are the ideal security technologies. Organizations tend to have the technologies in place that they desire, but this could be improved further. Advanced technologies are becoming more accessible and common than ever before; organizations should be adopting them before they fall behind their competitors or face a severe data breach, as so many have already.

## IoT security tools use and preference

Analysis of decision maker respondents whose organization currently uses to secure its IoT data/services/devices compared to ideal use.




Split by respondent type, asked to all respondents (1,050 decision maker respondents and 10,500 consumer respondents)

# Consumer impact on security

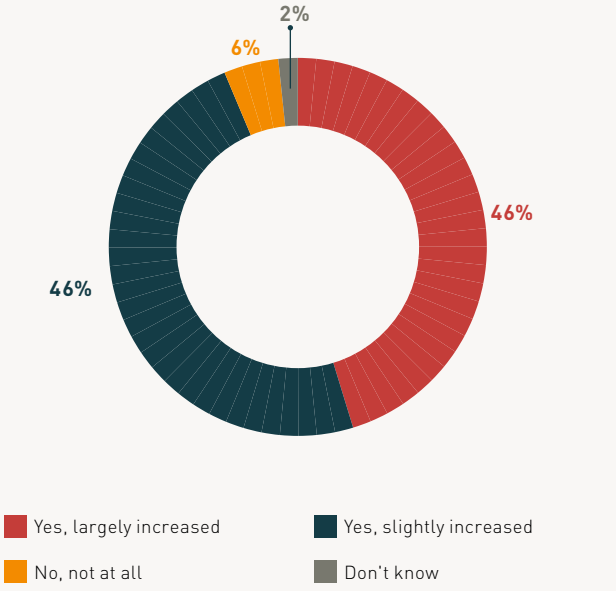
Justifying spend on security can often be difficult. But, that shouldn't be the case. Almost all (97%) decision makers, whose organization is an IoT enabler, think that security is a consideration for their customers when they are using their IoT products/offerings. Slightly fewer (82%) consumer respondents do say that security is a personal consideration when using an IoT product. The vast majority of both respondent types see security as important, which should go some way to justifying that investment. However, nine in ten (90%) consumers expect IoT security to come as standard, rather than as something that they would have to look into or consider themselves. This can leave a dangerous gap in the security of their devices. Ultimately, leaving devices unsecured can lead to consumers facing theft of personal information, banking details or identity fraud.

The importance of IoT security is clear. More than nine in ten (92%) decision makers whose organization provides IoT manufacturing, software or services think that their organization has seen increased sales/product use due to their IoT security. Security does appear to play a part in consumers' decisions, whether consciously or not, and should encourage organizations to make that initial investment in IoT security and drive organizations forward in their journey. If organizations do not get security right, they will not build or retain their customer base.

> Security does appear to play a part in consumers' decisions, whether consciously or not

**Security as a sales tool**

"Do you think that your organization has seen increased sales/product use due to its IoT security?"




Asked to respondents whose organization provides IoT manufacturing, software or services (600 respondents)

# IoT Partnerships

To maximize the potential of IoT, partnerships between organizations are vital. Almost all (95%) decision makers say that their organization partners with other organizations regarding IoT. These organizations partner with three other vendors, on average. Around half partner with cloud service providers (52%) or IoT service providers (50%), while nearly a third (31%) partner with IoT security specialists. Partnerships are most likely to be formed due to the partners having IoT skills/knowledge that organizations do not have (47%) and to facilitate and speed up IoT deployment (46%). Using partnerships can increase the complexity of the IoT ecosystem. But, for many, a partnership with a recognized IoT security specialist could pave the way for organizations to monetize their IoT solutions.

IoT partnerships can still be improved upon. Of decision makers whose organization partners with other organizations for the purpose of IoT, only a third (33%) report having complete control when their data moves between partners. However, almost six in ten say that better guidance from IoT security experts (57%) and more transparency over data security (55%) could help their organization improve the way that it partners. Security can dictate the success of an organization's IoT usage and having the right partners can give them the edge in offering a secure platform and offering the best possible customer experience.

When considering partnerships with other organizations in relation to IoT security, nearly all (96%) decision makers feel that their organization has/would see benefits as a result. Reduced costs (46%) will help validate any investment in setting up the partnership, while a better collaborative knowledge of IoT (38%) and increased customer confidence of IoT security (37%) will only improve the customer experience overall. The IoT ecosystem is ever growing, becoming more complex and more competitive; organizations need to get these partnerships set up and working to their full potential as quickly as they can.

**Benefits of IoT security partnerships**

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


Asked to all respondents (1,050 respondents)


Partnerships are most likely
to be formed due to partners
having IoT skills/knowledge
that organizations do not have.

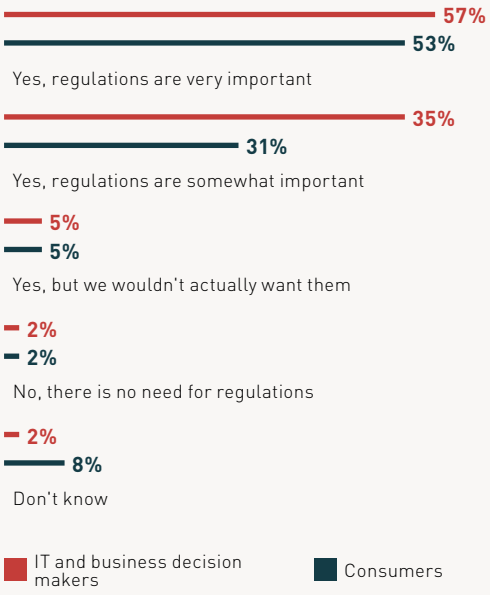
# Government regulations and impact

Regulations are a huge part of modern life, particularly in the world of technology and why should IoT be any different? The vast majority of decision maker (96%) and consumer (90%) respondents state that there should be IoT security regulations. In addition, a large majority of both decision makers (79%) and consumers (72%) agree that government intervention is important to IoT security. On the whole, guidelines and regulations would be welcomed into the IoT ecosystem. If consumer confidence in IoT security can be improved through regulations, then this will continue to drive IoT adoption and offer a huge opportunity to organizations; all organizations need to do is take that opportunity.

Security regulations often have to cover a wide range of scenarios and impacts. Around two thirds (65%) of decision makers, who think that there should be IoT security regulations, say that the security methods to be used for data storage should be included within IoT security regulations. In addition, just over six in ten (61%) believe that who is responsible for securing data at each stage of its journey should be included, while over half (55%) say the same for the implications of not complying. Partnerships with an experienced IoT security provider will become even more critical if, and when, IoT regulations come into force.

**IoT security regulations**

"Do you think there should be regulations in place regarding IoT security?"




Split by respondent type, asked to all respondents (1,050 decision maker respondents and 10,500 consumers)

# The consumer world of IoT

Thinking specifically about consumer respondents, more than half (54%) own an IoT device and they own four IoT devices, on average. There is evidently a consumer market for IoT devices; however, only just over one in ten (14%) consumers perceive themselves as being extremely knowledgeable about IoT device security. Poor IoT security can have huge implications across modern life. With so many everyday consumer devices becoming IoT enabled, a security gap in one could lead to a consumer's entire IoT ecosystem crashing down.

IoT based partnerships and security regulations could be critical to the future of IoT from a consumer perspective. Almost nine in ten (89%) consumers have concerns about IoT security, with a hacker controlling devices (65%) being the most common. Customer data being leaked (60%) and hackers accessing personal information through IoT devices (54%) are also big concerns. These fears could be as a result of the vast media coverage that cybersecurity breaches have gained, such as the recent WannaCry attack. In order to regain consumer faith in IoT security, organizations need to be able to prove that they have the right security partnerships and technologies in place, as well as an outstanding record for IoT security.

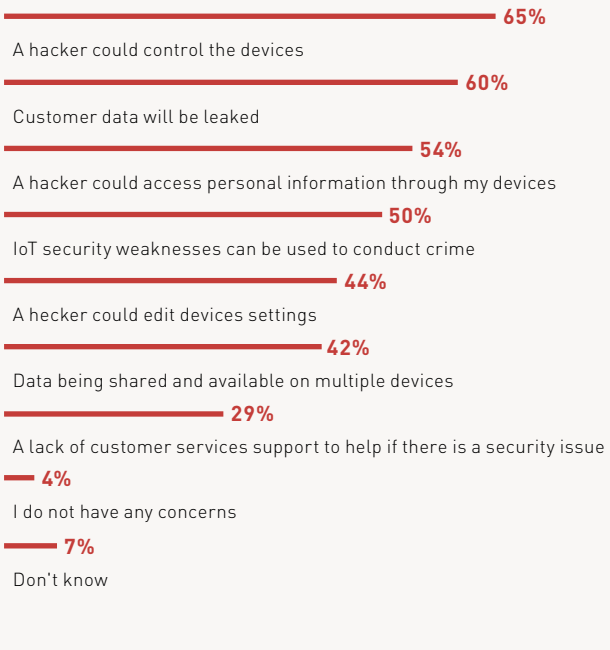
The level of security required for different IoT devices is likely to vary, according to consumers. Over half believe that connected cars (54%) or smart cities (51%) require advanced levels of security, compared to under a quarter (23%) who think this about health and fitness devices. However, leaving any device unsecured is alarming, particularly as IoT devices require and capture more data than ever.

Consumers expect IoT devices to come secured as standard and are fearful over the safety of their data. But, in reality, organizations who store data or use IoT devices are not doing this. Only 57% encrypt all of the data that they store or receive. Additionally, only around six in ten of those who do encrypt, do so as soon as data is captured on the IoT device when it comes to data that they store (62%) and data that they send (59%). This should cause mass concern. Fewer than half (45%) of consumer respondents who own at least one IoT device have changed the default password on all of their IoT devices. IoT devices will often be sold with basic passwords, if they even have one at all.

Ultimately, consumers need to be able to have faith and trust in IoT security. This being possible will depend on the involvement of IoT security specialists. When it comes to who is in the best position to protect IoT users' data in the cloud, consumers are most likely (31%) to state that a well-established company that specializes in security would be in the best position to protect that data. IoT partnerships are important for organizations to offer the right level of IoT security and this is mirrored in consumer beliefs. Organizations will continue to monetize IoT through strong security and how better to display that, than a partnership with a well-established IoT security specialist?

**Concerns with IoT security**

"What concerns do you have when it comes to IoT security?"




Asked to all consumer respondents (10,500 respondents)

# Organizations and governments can no longer afford to neglect IoT security

Consumers want more, expect more and need more. Dynamic changes in technology are creating seismic shifts in the way that organizations operate. In addition, digital consumers are becoming increasingly empowered with an increase in technology at their fingertips. This all leads to a complex ecosystem within the technology world. Organizations need to be able to connect with technology, and each other, to ensure that they keep pace in this digital era.

In particular, the utilization of IoT can be the key to unlocking the door between organizations and a successful and prosperous future. IoT is here to stay. It can enable organizations to securely offer new services, become a revenue driver in itself and improve customer experience. All being reasons to pursue an IoT journey.

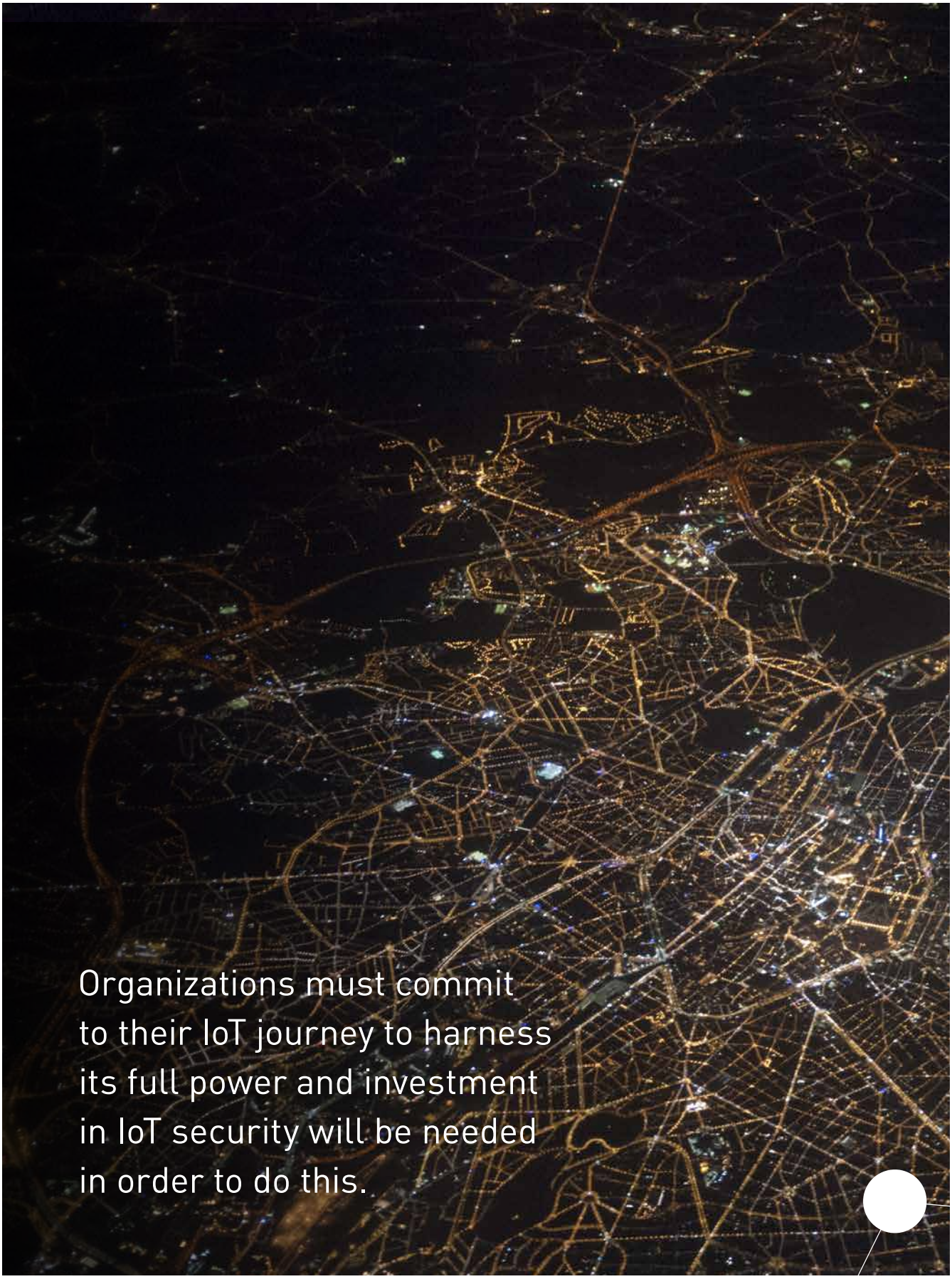
Are there challenges to adopting IoT? Yes, of course. It's no secret that IoT can divide opinion, with security being a key reason for some initial skepticism. But, there are ways to overcome these reservations, with mandatory regulations being one of them.

Organizations must commit to their IoT journey to harness its full power. Investment in IoT security will be needed in order to do this and must continue to happen. Understandably, consumers can be concerned over the security of their devices and data. For most, it's a consideration when choosing which devices to use and it can be a vital selling point for organizations.

The IoT ecosystem is complex and the journey can be long. But, the optimization of IoT could be best seen through organizational partnerships. Achieving consumer confidence could be best seen through partnerships with an experienced IoT security specialist.

IoT is not going away and the sooner organizations can offer a secure platform the better. Organizations need to see the warning signs and act upon them – IoT related breaches can be excruciatingly costly. And let's not forget the consumer. With the number of IoT devices becoming available, security is becoming a differentiator for them. So, can organizations afford to neglect IoT security any longer?

TO LEARN MORE, VISIT: WWW2.GEMALTO.COM/IOT


Organizations must commit
to their IoT journey to harness
its full power and investment
in IoT security will be needed
in order to do this.

## About Gemalto Enterprise Security

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.

Powered by gemalto