Benefits and challenges of IoT in business

With superpower comes super responsibility

kaspersky BRING ON THE FUTURE

Learn more on www.kaspersky.com

Contents

Introduction

The use of Internet of Things (IoT) devices in business is growing at an exponential rate. According to Gartner, the number of global IoT connections is expected to rise to approximately 25 billion by 2025.

Simply put, IoT covers every device connected to the internet, from wearables to industrial sensors. It is increasingly being used to define connected objects that 'talk' to each other through sensors with the capacity to collect data and use it to make business more efficient and our lives easier.

Initially suggested as a way to improve organizational processes, IoT devices have quickly become a way of enhancing our personal lives as well. While this led them to gain popularity in devices such as smartphones, watches and voice assistants, they still have a strong impact in organizations.

Here, connected devices impact nearly every business industry, with devices including machine learning for predictive maintenance, smart grid, sensors for shipping and logistics, automated manufacturing process, and connected HVAC (Heating, Venting, and Air Conditioning) systems among others. These allow for data collection, exchange and analysis of many more touchpoints across the full set of business processes.

With the addition of large volumes of data from all these elements, businesses can gain actionable insights to help them better understand their workflow, drive productivity and increase efficiency – as well as ultimately transform their business processes. As well as streamlining existing businesses, organizations are able to consider potential new directions, development of new products or services and expanding lines, all thanks to IoT capabilities.

Yet, with this rise in connected devices also comes increased need for security. Gartner has highlighted that nearly 20% of organizations have already observed cyberattacks on IoT devices in the past three years. Because of their levels of connectivity and access to business networks, IoT systems increase the potential cyberattack surface at any organization. Therefore, the most important consideration for organizations looking to introduce IoT devices into their business processes is to ensure they provide strong IoT system security.

As IoT solutions increasingly emerge in businesses, industry and even local government, the need for increased security is set to grow. Therefore it's vital that organizations raise their levels of awareness in IoT security and the ability to mitigate risk.

This report helps technology suppliers, service providers, organizations and security professionals who are planning (or already implementing) IoT systems to understand the growing IoT landscape. It looks at the range of opportunities that IoT offers for organizations, along with the challenges these new systems present. It also provides cybersecurity recommendations for IT security professionals to follow, to make the most of their IoT platform and secure it from potential data breaches and attacks on the whole network.

Key findings

1. The use of IoT is already widespread across a range of business industries: **61% of organizations** are currently using IoT platforms in their business.
2. IoT use is even higher in the IT and telecoms **industry (71%)** and **finance (68%)**
3. The growing rate of IoT increases the business need for data protection and prevention from cyber-incidents. In the first half of 2019, Kaspersky researchers detected **105 million attacks** on IoT devices through honeypots.
4. Nearly three-in-ten **(28%) companies** using IoT platforms experienced incidents involving non-computing connected devices in the last year.
5. The reliability of suppliers is no less important, with more than a third **(36%) of companies** giving third parties access to their IoT platforms.

Methodology

The findings in this report are taken from several sources including: the Kaspersky Global Corporate IT Security Risks Survey – formed of a total of **4,958 interviews** with IT business decision makers, conducted across **23 countries** in 2019; Kaspersky's threat research into attacks on IoT devices through honeypots and Kaspersky ICS CERT research on the threat landscape for smart buildings; and Kaspersky's security assessment of corporate information systems report.

In addition, statistics are included from third party sources, including Gartner, IDC and GSMA, and Cybersecurity Insider reports.

Superpowers demand responsibility: the collision of efficiency and privacy in IoT

More data, more efficiency

The role of IoT in business has grown rapidly in recent years. Today, IoT systems can be used to introduce cost reduction and savings to businesses, as well as unlock new revenue streams and make production processes more transparent.

According to Kaspersky's survey, **61% of organizations** currently use IoT platforms as business applications. In fact, there are actually several industries where their use of IoT is even higher: **71% of those in the IT and telecoms industry** use IoT, while **68% of those in the finance** world follow suit. Meanwhile, at utility and power companies, this figure is **two-thirds of businesses (66%)**.

Year-on-year use of IoT platforms by industry

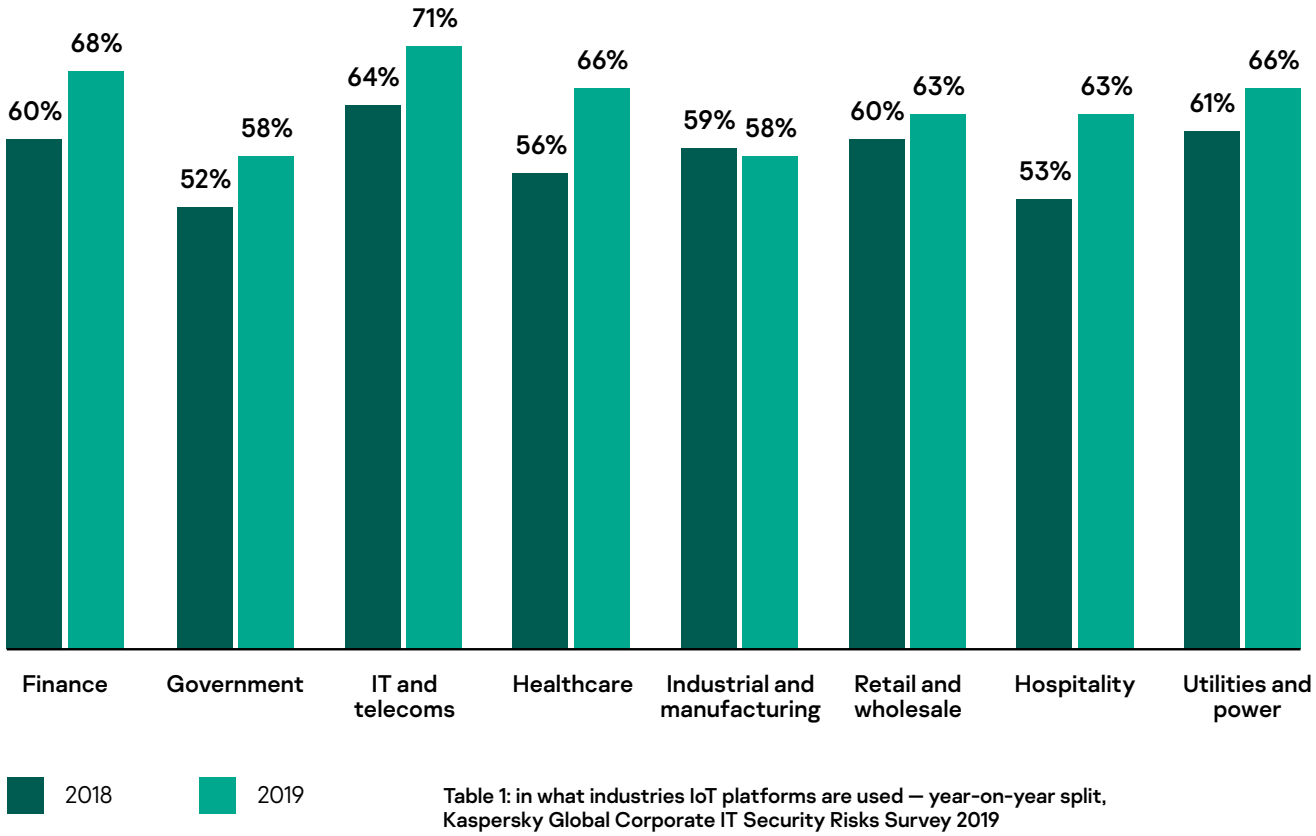

Table 1: in what industries IoT platforms are used — year-on-year split, Kaspersky Global Corporate IT Security Risks Survey 2019

Notably, total IoT spending is set to reach **$1.1 trillion** by 2025, jumping by a huge **567% up** from **$166 bn** in 2016, according to forecasts from GSMA and IDC. This impressive growth is likely due to the wider levels of use of IoT across business, industry and sectors such as city planning. In fact, we are already starting to see IoT used for connected transportation, industrial automation, the automotive industry, the wider deployment of smart city initiatives and more.

Smart cities

Singapore is one example of a city aiming to transform the quality of living through technology. In recent years, it has implemented road sensors that connect to phased traffic lights and smart parking systems, leading to significant improvements in traffic management.

Meanwhile, Barcelona is aiming to tackle city-wide environmental concerns though smart streetlights and sensors monitoring air quality and noise, which connect to smart grid pilot projects and smart household meters.

According to IoT Analytics, the number one growth area for all IoT projects globally is in the use of smart cities. In smart cities, local authorities can utilize connected IoT devices to introduce systems such as street lights, smart parking and smart utility meters for offices and households. The prospect of IoT systems widens from simply running utilities management for residents and lighting controls to critical services such as transportation management, traffic control and video surveillance.

One of the main triggers for this growth of IoT in smart city projects is the need for cost reduction. Being able to monitor and optimize public systems and services through smart devices allows local authorities to best utilize resources, such as energy or water, helping to save money across these new developments.

In addition, the growing penetration of 5G, one of the most discussed topics in tech right now, will also enable significant growth of IoT in smart cities as it rolls out higher network bandwidth.

This promised high speed wireless technology will enable the transportation of far larger volumes of data and reduce response time across mobile networks – all allowing for the wider use of IoT applications and the transfer of data from city-wide smart sensors.

In Europe, 45 new '5G trial cities' are expected to be launched in 2020, including London, Ghent, Paris and Berlin, to host and demonstrate use cases for the technology. They will begin implementing 5G across vast urban locations to test the potential for development in smart cities, such as in energy, transport, smart buildings and digital-health platforms.

Despite these trials, the full implementation of 5G mobile networks at a national, or city level, may take longer than telecoms providers originally predicted. China for example, currently one of the most advanced 5G nations, now estimates a time frame rising to 2030 for the final developments of a country-wide 5G network.

Industry and manufacturing

But it's not just in futuristic smart cities where IoT is leading to business efficiencies. Thanks to the intelligence and monitoring that IoT devices offer, industrial organizations can gain increased transparency and the opportunity for automation, or predictive maintenance.

In Industrial IoT (IIoT) technology, sensors can be attached to machines. During the manufacturing process, those sensors gather data, analysis of which helps manufacturing owners take action.

The World Economic Forum recently recognized a number of organizations it considers "beacons of technology and innovation in manufacturing". Each of them use an IIoT infrastructure to advance their business processes, including big data decision-making, democratized technology on the shop floor and new business models. One of these recognized organizations, Tata Steel, uses IoT sensors across its IJmuiden plant in the Netherlands to solve industrial problems. Analysis of this data has helped the organization optimize the way it uses raw materials, increase its yield and find solutions for waste reduction across the manufacturing process.

"Digital transformation is about transforming an entire business from the culture to the strategy to the goals. IoT, and especially Industrial IoT (IIoT), is critical to digital transformation across industries. The Precision Crop Management Testbed is an **example** of this transformation, which uses IoT technology (sensors) to improve crop productivity (yield)," commented Dr. Richard Soley, Executive Director, Industrial Internet Consortium.

Interestingly, in the case of IIoT, one main engine driving smart projects is manufacturing equipment vendors who are looking to provide transparent, efficient processes to their customers. Thanks to IoT smart metering, they are able to run visible product lifecycle management which shows how each piece of equipment is being utilized. Based on this data they can then offer new ways of manufacturing optimization, such as detecting abnormal patterns in an asset's performance or establishing where in a workflow the productivity drops, and why.

On top of this, vendors can now offer their customers new solutions such as 'equipment as a service' — where a customer pays based on working cycles or productivity, instead of buying or renting the equipment itself.

The question of privacy and data safety

Because of their connected nature, IoT systems involve many components which vendors and third-parties may need to access. For example, in smart city projects, systems such as traffic controls, CCTV and even utility supplies to apartments, store many different types of personal user data. Therefore, it's important that the smart system is configured and protected to ensure this data cannot be unlawfully accessed.

According to Kaspersky research, **36% of companies** admit that third parties have access to their IoT platforms. This is higher than for many other elements of business infrastructure, such as **office productivity software (23%)**, **email (27%)** or **enterprise resource planning (ERP; 30%)**.

One notable case illustrates why connections with third parties should be given consideration in terms of data security. In 2019, Kaspersky ICS CERT experts conducted **research** into threats to smart building automation systems. The findings show that on **38% of computers** in the automation systems of smart buildings, malicious objects were detected and blocked.

Access to business applications by third parties

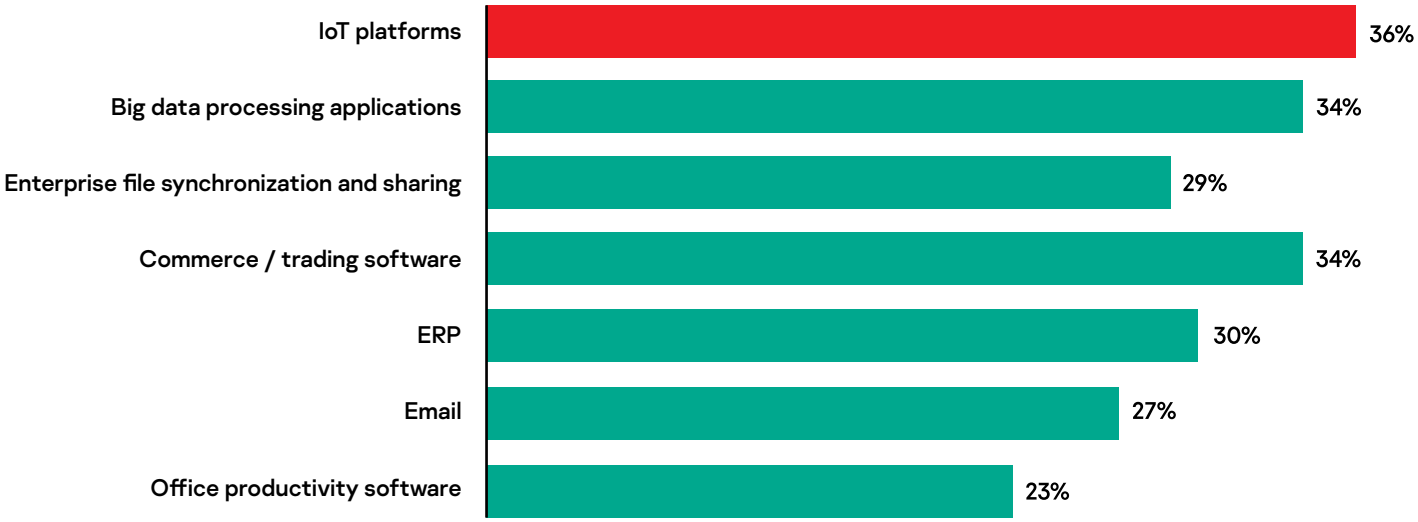

Table 2: what business applications are accessed by third parties, Kaspersky Global Corporate IT Security Risks Survey 2019

Among the attack vectors researchers found a remarkable instance of one conducted through a contractor that supplies building automation systems to different organizations. An attack to this contractor with backdoors and spyware would allow threat actors to gain remote access to facilities where these systems are being used, such as smart building systems in airports, transportation hubs or office buildings.

As well as ensuring the reliability of third parties who have access to IoT systems, it is important for organizations to think about the security of these devices. This is highlighted by the **28% of companies** using IoT platforms who stated that they experienced incidents involving non-computing connected devices in the last year. This is higher than **those affected by crypto-mining attacks (26%)**, **incidents involving data-sharing suppliers (27%)** and **infrastructure incidents involving third-parties (27%)**.

Given their connected nature, IoT platforms unite many different devices on one network, each of which can become an entry point for an attack, causing the overall attack surface to widen. Therefore it is important for businesses and IT security professionals to consider the challenges and concerns that may arise with IoT implementation, as laid out in the next section of this report.

Incidents experienced by organizations using IoT platforms

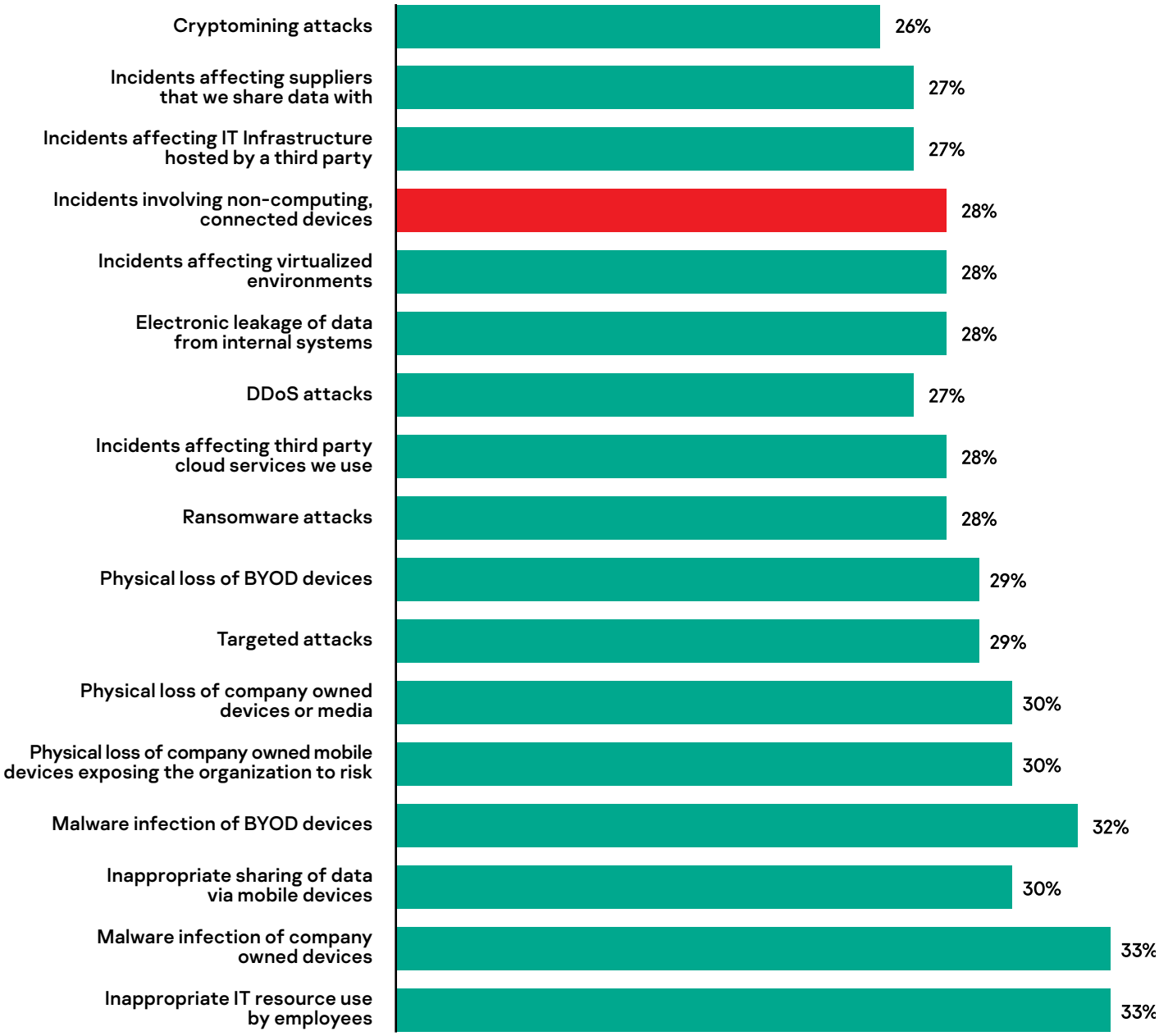

Table 3: what incidents are experienced by organizations using IoT platforms, Kaspersky Global Corporate IT Security Risks Survey 2019

Superpowers don't come without challenges: what to prepare for when implementing IoT

Businesses are in clear need of IoT processes

Although the technology behind IoT is at a high level, and devices are already in use in many different industries, there are certain areas where IoT project implementation demands greater efforts and attention.

"For example, in smart city projects, there can be challenges with the fragmentation of IT systems behind the smart network. Often different city services and departments use different platforms and applications, making it harder to roll out systems across diverse networks. In cases such as this, there is often no one unified IT platform, nor a single management and decision making process. As a result, a project to connect different city IoT services together can require more resources to complete," said Marat Nuriev, IoT Security Business Development Manager at KasperskyOS Business Unit.

This reflects a study by Gartner, who found that more than **a third of security professionals (38%)** believe the top security challenge for IoT is poor visibility and understanding. In addition, a **lack of standardization (22%)**, and poor support and practices for IoT are affecting IoT structures in their business.

The growing need for expertise at the junction of industrial processing and IoT

In some cases, the implementation of IoT systems also demands specific expertise that an organization may not have internally. The solution here will come from additional human resources or an external service provider, who can bring knowledge and support to an organization and help them establish dedicated business processes.

"In situations where external expertise is needed to implement IoT systems, some businesses and industrial organizations in particular, may be reluctant to trust external or third-party experts, if they feel they are not savvy in specific manufacturing processes – whether that is steel casting, assembly of equipment or food production. As industrial manufacturing is so diverse, customers today are looking for specialists who know how their industry works in each specific case, as well as how IoT should be implemented to best fit the company and the solution needed," Marat commented on the trend.

Trustworthiness and identity

According to Dr. Richard Soley, Executive Director, Industrial Internet Consortium, "**Trustworthiness** is an all-encompassing term that is central to the **mission** of the IIC. Safety, privacy, reliability and resilience need to be considered in conjunction with security to establish that IIoT systems will be trustworthy, i.e., functional, but will also not harm people, the environment or society".

"More importantly, trustworthiness driven by identity, has pushed us to explore blockchain or (DLT) distributed ledger technology – an immutable time-stamped series record of data that is distributed and managed by cluster of computers. Identity is central to a trustworthy IIoT and the ecosystem around it. DLT technology enables a decentralized trust model for interoperable digitized identities of physical goods, documents, immobilized assets, sensors, and machines. DLT has the resiliency to scale to support billions of connected devices".

"In 2020, we'll see a blossoming of non-centralized, IIoT systems taking advantage of DLT, identity and artificial intelligence technologies. Certifiable models based on the IIC reference architecture, connectivity architecture, trustworthiness and other results will drive international standards, which is already happening," concluded Dr. Soley.

What is important to know about IoT cybersecurity?

Cybersecurity is an important area of focus for organizations implementing IoT projects. In an attempt to acknowledge this, some IoT vendors now offer suites of 'secure IoT platforms' which boast in-built protection from cyberthreats.

However, historically, the task of protecting against cyberattacks has not been paramount in the development of smart devices.

"Firstly, in-depth protection requires additional investments, which would increase the cost of the device. Besides, various smart devices and sensors have very limited computing power and should consume little energy. In this case, the security of the system can be ensured at the level of the secure IoT gateway to which all IoT objects are connected, and through which they transmit information to a data center for processing," commented Evgeny Goncharov, Head of Kaspersky ICS CERT.

"Secondly, so far not many high-profile attacks on IoT have been investigated that would catalyze the mass adoption of a security layer to device development. This doesn't mean however that threats to IoT do not exist. IoT provides the potential possibility to use a network of smart devices to create botnets (as was the case with the **Mirai botnet**), or to gain access to data the IoT system collects, or to other systems that various parts of the IoT platform are connected to," added Evgeny.

Kaspersky researchers **have recently detected** **105 million attacks** on IoT devices through honeypots – networks of virtual copies of various internet connected devices and applications. This figure accounts for the first six months of 2019 and is seven times greater than the number of threats found in H1 2018.

To avoid the repetition of the WannaCry story for IoT, it's important that vendors consider cyber-protection within their products, and that customers become responsible for the process of building a secure industrial IoT system which is kept up to date. To minimize the risk of a cybersecurity incident in IoT, businesses should therefore make sure their overall network and devices are secured properly and software is updated in a timely manner.

Cybersecurity decision-making

Kaspersky experts have undertaken various cybersecurity assessment projects in the field of IoT. According to their findings, when it comes to improving the cybersecurity posture of IoT and networks, one of the main obstacles for organizations is the lack of decision-making power at cybersecurity department level. Insufficient cyber-protection maturity is often connected with management issues, when a cybersecurity team doesn't have enough influence on C-level decision makers.

This can lead to a situation where a company doesn't take decisions that are important for cybersecurity — for example, establishing specific processes or purchasing additional security systems. Or decisions made may be unreliable in terms of cybersecurity, such as purchasing equipment of inadequate quality or working with unreliable suppliers. While the overall level of protection — not just IoT but the entire IT security provision — is low or extremely low in **43%** of companies they **analyzed**, the decision-making process is the thing that companies need to work on.

IoT data and the cloud

Given the additional levels of data generated by IoT, businesses now need better, more efficient ways to store and process this data. Therefore, systems can be connected to the cloud where data from different smart devices can be collected and passed for processing. Of course, customers can choose to use either a private or public cloud platform to best suit their business needs. Public clouds offer advantages for IoT because applications for data processing which may be run in the cloud can help transform gigabytes of telemetry into clear data visualizations showing device operations and efficiency.

Although public cloud providers promise protection for their platforms, some companies still doubt the security of these services (**93% of security professionals**, according to a report by **Cybersecurity Insiders**). Ultimately, the security of public clouds is a matter of management. Risk of any incident can be minimized if a provider guarantees protection of its entire cloud platform, as well as the security domain separation for its various customers and services. In this way a compromise to one customer service could not affect other customers and services. In addition, customers should utilize the necessary tools to secure their on-premises and in-cloud workloads and ensure proper configuration.

Takeaways for your IoT journey

IoT offers huge potential for organizations to transform manufacturing processes, business growth and even the cities in which people live. As the amount of data that organizations have access to increases, so too does the ability to develop insights and understand how to improve business efficiency.

Yet, while IoT brings these and many more benefits, businesses must also be aware of the cybersecurity objectives. Risks can include outage of services, data loss regulatory incompliance, reputational and direct financial loss. All of these provide challenges to businesses who may not yet have put dedicated IoT security policies in place, or struggle with IT security budgets.

Importantly, these can all be managed with the right attention to cybersecurity processes. For many organizations who are only just starting to build their IoT solutions, any solution they invest in for security must provide scalability as their networks grow, as well as context for IT security professionals to easily monitor threats to the network and action fixes.

As the connectivity of everything becomes the new normal with IoT, networks which were once isolated become a wide area network. This means the security landscape is much broader – stretching from not just individual device security, but to network security, which needs protection at the infrastructure level.

IoT security must be ensured at all levels: product development, customer implementation, and regulation. The development of secure IoT devices can be carried out on the basis of secure operation systems and platforms, and IoT-specific security functions should be implemented in the classical security solutions for IT and telecom systems. There are already industry practices of developing IoT security recommendations based on threat assessments, and they need to be supported by the community and governments.

To securely take advantage of all the features and benefits of IoT, Kaspersky suggests organizations follow these steps:

1. **Assess the status of a device's security before its implementation.** Preferences should be given to devices that have cybersecurity certificates and products of those manufacturers that pay more attention to information security. The Industrial Internet Consortium created a special **framework** that can be used to research and certify IoT / Industrial IoT devices for information security.

2. **Conduct regular security audits and risk assessments,** and provide the security team responsible for protecting IoT systems with up-to-date threat intelligence. This is important in IoT systems, as well as the overall IT infrastructure.

3. **Regularly update your list of all partners and suppliers**, as well as the data they can access. Ensure that organizations that no longer collaborate with your company cannot access or use data and assets. Provide all third parties with the requirements they should follow – including compliance and security practices.

4. According to Kaspersky's **security assessment report**, **86%** of analyzed companies had obsolete or vulnerable software. Therefore, **it is very important to update software and applications**, and security solutions on all devices and parts of the IoT network.

5. **Establish procedures for obtaining information on relevant vulnerabilities** to ensure proper and timely responses to any incidents. When choosing IoT solutions for integration, if possible, prioritize those that allow you to update software based on root of trust.

6. Researchers also found that a corporate network is sometimes used as a communication channel between smart devices and the data center. To secure your business-critical assets, **implement cybersecurity solutions** designed to analyze network traffic and detect and prevent network attacks covering traffic from IoT devices, and integrate the analysis into the enterprise network security system.

7. **Use IoT devices that are secured by design.** While many gateways are described as 'secure' or 'trusted', many actually only protect IoT devices connected to the gateway, rather than protecting the gateway itself. This means that if the gateway becomes compromised, all the security technologies can be deactivated, and all IoT devices on the network will be affected. The **Kaspersky IoT Secure Gateway** with secure KasperskyOS at its core ensures the secure behavior of the gateway itself, as well as all connected devices and the entire IoT system.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky