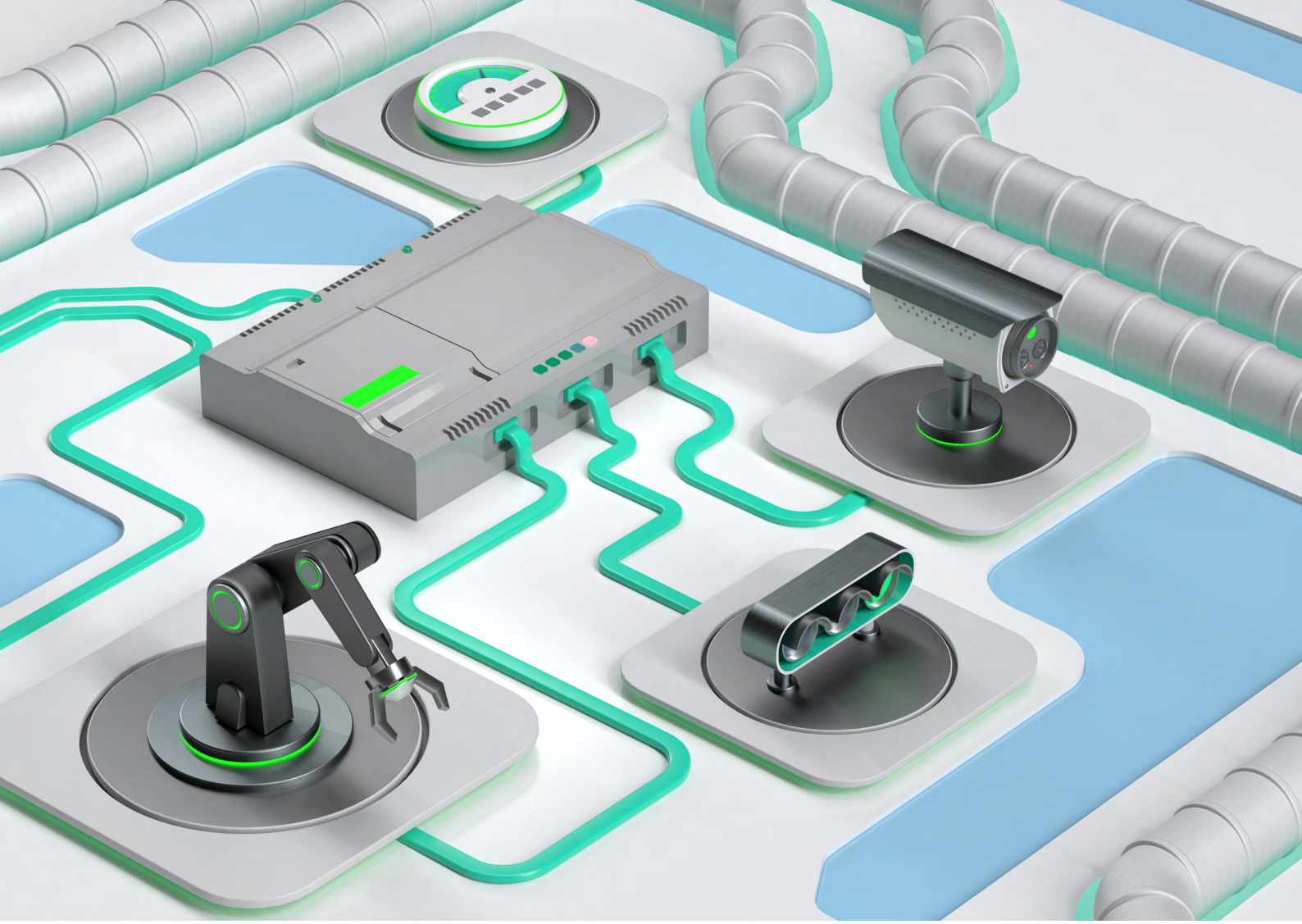


Pushing the limits: How to address specific cybersecurity demands and protect IoT

IoT Report

kaspersky BRING ON THE FUTURE

Learn more:
kaspersky.com

Contents

Introduction

The Internet of Things (IoT) describes the increasingly sophisticated, complex network of online, connected devices that enhance our cars, homes, and cities. According to IoT Analytics, the global number of connected IoT devices is expected to grow 9% and achieve 27 billion IoT connections by 2025.

From smart homes and cities, driverless cars, and pollution control to the transference of data to monitor important processes and provide new insights, boost efficiency, and allow companies to make more informed decisions – the fast growth of IoT is changing the way we live and work.

With the dramatic rise in connected devices also comes an increased need for security. In fact, Gartner highlights that nearly 20% of organizations have already observed cyberattacks on IoT devices in the past three years. Addressing cybersecurity risk can help companies leverage IoT opportunities while tackling the vulnerabilities that are part of the latest regulatory guidance. **Regulatory bodies and government organizations worldwide are realizing the dangers and risks of connected devices that are not built with proper security in mind** — and responding with a variety of regulations for which companies will be forced to comply.

As we highlight in the first part of our report below, complex or innovative projects, such as IoT, have specific security requirements that traditional security tools do not always provide. The development environment and the variety of device types add even more complexity to protecting IoT against threats.

This report aims to help technology suppliers, service providers, organizations and security professionals who are planning or already implementing IoT systems to understand the growing IoT landscape.

It also starts a dialogue on how Kaspersky Cyber Immunity approach can help to secure IoT platforms from potential data breaches and attacks on the whole network to reap the rewards without the risks.

Methodology

The Kaspersky Corporate IT Security Risks Survey (ITSRS) is a global survey of IT business decision makers

The Kaspersky Global Corporate IT Security Risks Survey (ITSRS) is a global survey of IT workers. A total of 4,303 interviews from businesses with more than 50 employees were conducted across 31 countries in May-June 2021.

Throughout the report, businesses are referred to as either SMBs, (small and medium sized businesses with 50 to 999 employees), or enterprises, (businesses with over 1,000 employees). Not all survey results are included in this report.

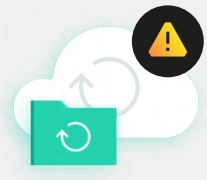
The report also includes opinion pieces by experts: Eric Kao, Director, WISE-Edge+ of Advantech, and Stephen Mellor, Chief Technology Officer at the Industry IoT Consortium (IIC).

Key findings

In 2021, **53%** of organizations abandoned new business projects due to an inability to address cybersecurity risks, and **74%** faced a situation where there was a lack of an appropriate security solution

64% of businesses already maintain or use IoT solutions

However, the risk of a cybersecurity breach is the biggest concern for **57%** of organizations that are planning to implement IoT



52% of organizations are worried about collecting big data from IoT devices because of the risk of cyber-sabotage and espionage

43% of businesses surveyed indicated that at least one type of IoT was not protected, highlighting a clear need for dedicated cybersecurity tools

Specific cybersecurity demands

When it comes to cybersecurity risk, no two organization or innovations are the same.

According to Siemens, cybersecurity is a rapidly changing battlefield that requires awareness, continuous vigilance, and a consolidated response from everyone involved. Cyber-protection is not a product that you simply invest in once and then forget about. It is an ongoing process.

Implementing the same cyber-risk controls everywhere and equally doesn't always work. Applying sectional protections that leave some vital information assets vulnerable while focusing too closely on less critical ones is also not a way out for enterprises adopting innovations such as IoT. Cybersecurity budgets, meanwhile, compete for limited funds with technology investments intended to make the organization more competitive.

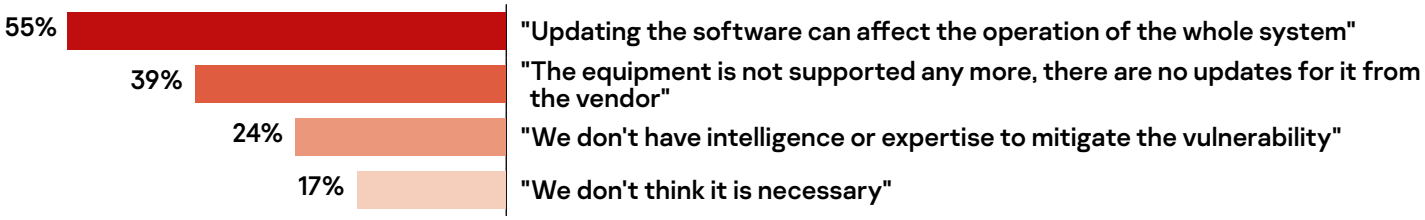
However, sometimes the issue is meeting very specialized cybersecurity requirements, which is not easy to do. In 2021, **74%** of companies faced at least one situation where there was a lack of appropriate security solutions, and **53%** abandoned implementing new IT solutions, updating corporate policy, or even launching a new business project because they were unable to address cybersecurity risks.

Figure 1: Key areas of business operations undermined due to security concerns

Looking broader, every second organization (**53%**) had to figure out troubles with their cybersecurity solutions. Our research found performance (**35%**) and maintenance (**34%**) issues were the most common ones. However, these should be expected just as with any other IT and technology. These routine tasks are followed by compatibility issues (**34%**) with specialized software or firmware, such as industrial and manufacturing. That said, IT security teams have to find compromises and workarounds.

We've all seen the importance of timely patching and software updates. However, this can present a significant problem too, with **28%** of businesses reporting vulnerabilities that are impossible to patch for the following reasons:

Figure 2: Problems with patching



The range of obstacles and challenges facing organizations implementing cyber-protection for IoT are exacerbated by the diverse set of industries in which they operate, as we will see in the next part of our report.

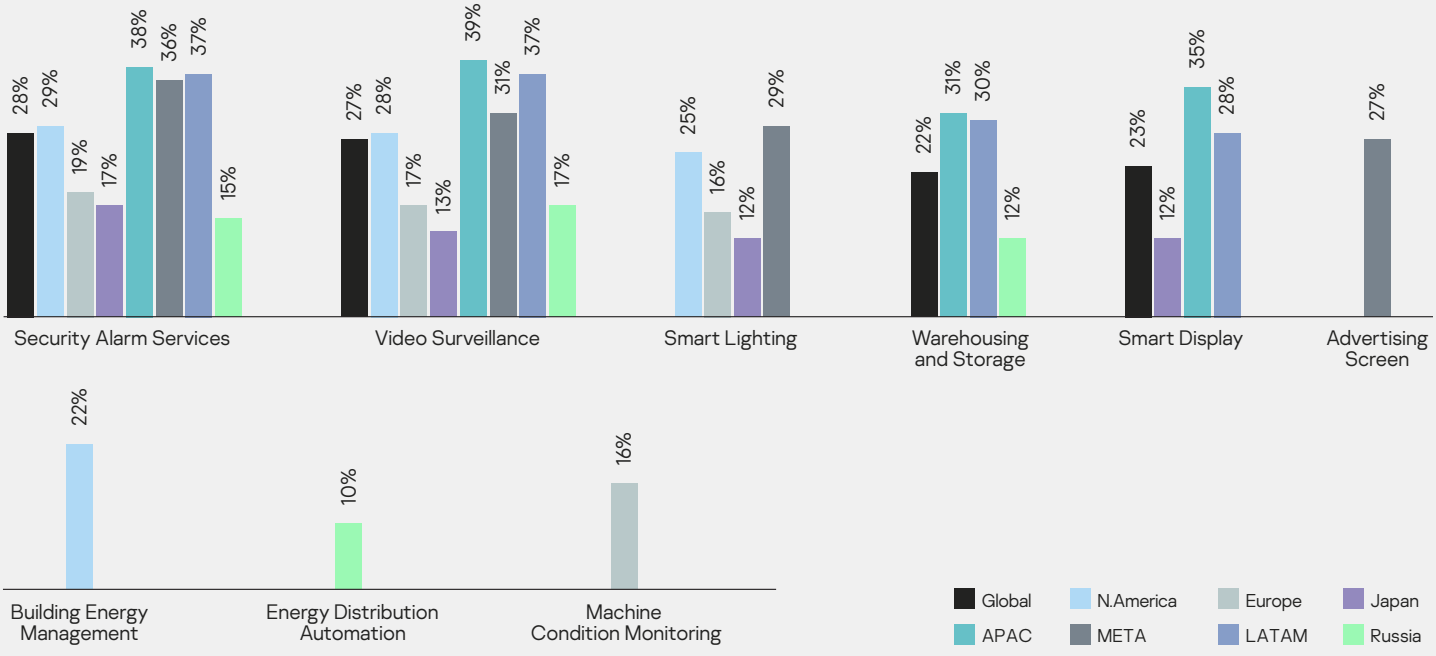
Reward vs. risk: Leveraging IoT solutions globally

IoT is widespread across a range of diverse business industries — from retail and transportation infrastructure to energy, industrial and smart cities. The type of devices also includes a vast array, such as video surveillance, security and alarm sensors, machine conditioning monitoring, EV charging stations and energy distribution automation (see Figure 3).

Figure 3: Global industry accelerates widespread IoT adoption

	Global	N.America	Europe	Japan	APAC	META	LATAM	Russia
Any Use of IoT	64%	68%	57%	57%	75%	72%	72%	41%
Retail	62%	N/A	55%	50%	75%	71%	71%	40%
Smart City	62%	67%	54%	N/A	74%	71%	71%	40%
Industrial	60%	N/A	52%	46%	71%	69%	70%	38%
Transport. Infrastructure	57%	N/A	50%	34%	71%	68%	67%	38%
Energy	49%	N/A	46%	25%	61%	61%	57%	26%
E-Health	N/A	6%	N/A	N/A	N/A	N/A	N/A	N/A

Percentage of companies planning to increase the use of following IoT solutions

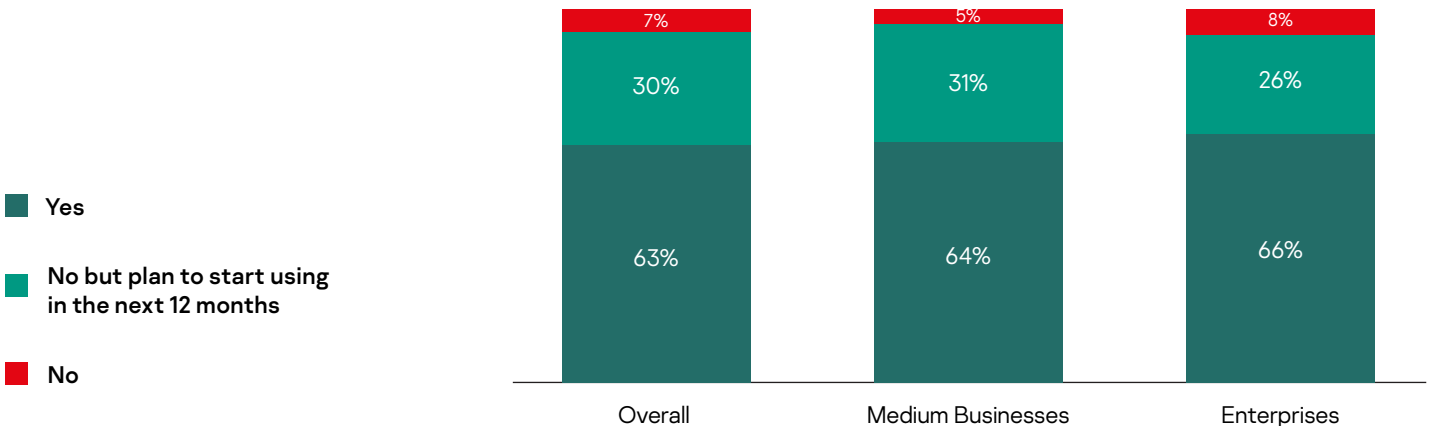


Overall, **64%** of businesses maintain or use an IoT solution. This rises to **68%** in the industrial and manufacturing sectors and **71%** in utilities and power. When it comes to gaining value from the information collected by the device, **63%** of organizations use big data or telemetry from IoT devices for business purposes. The manufacturing sector leads the way here (**65%**), closely followed by utilities and power (**62%**).

IoT devices are used in a wide range of businesses and industries and are ideal for making the most of data analysis. These devices contain chips, cameras, sensors and many other components that receive and collect huge amounts of valuable data. Analysis of this data helps to improve the efficiency of equipment, predict anomalies or damage, and find the most optimal way of organizing manufacturing process

Russian Chelyabinsk Pipe Rolling Plant (ChelPipe) is a major player in the Russian metallurgy market and a leading domestic producer of steel pipes. ChelPipe plant's engineers piloted an IoT gateway by Aprotech and Siemens MindSphere cloud solution that allowed them to collect data from industrial sensors and process in a cloud application. With that information, they can resolve a number of key issues — for example, determine what factors, under conditions that were otherwise equal, cause a change in the process indicators. Armed with this information, they can make operational decisions practically, and immediately in real time.

Figure 4: How IoT and big data connect across industries



Unfortunately, many IoT devices have little or no protection at the software and infrastructure levels. They are often unsupported and have no updates from the vendor. Implementing IoT solutions on top of existing legacy systems, which were once standalone and unconnected, will also create vulnerable targets for cyberattacks.

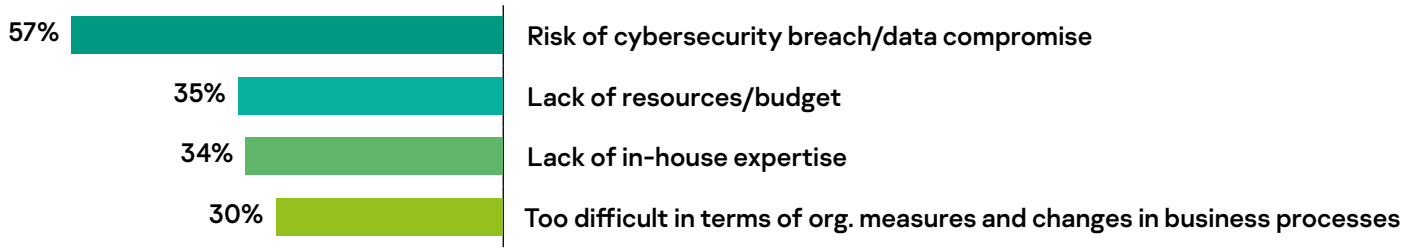
Exercise equipment maker, **Peloton** hit the headlines earlier this year, when a data breach appeared to stem from an exposed API that allowed anyone to pull up the private information of Peloton members, including those with the most private data settings.

Another example is an **attack** on surveillance startup, Verkada, which resulted in criminals gaining access to 150,000 surveillance cameras in hospitals, schools, prisons and companies. It is said that attackers were able to obtain access to cameras with a 'super admin' account that had been publicly exposed on the Web.

Indeed, despite the growing rise of IoT, more than half of the organizations we surveyed are concerned about cybersecurity breaches and data compromises when implementing IoT (**57%**). A lack of resources or budget constraints is cited as the second reason by a wide margin (**35%**).

When it comes to different industry worries, **53%** of companies in the industrial sector are concerned about a cybersecurity breach and data compromise risk, followed by a lack of in-house expertise (**35%**). The utilities sector shares a similar concern, with **50%** and **44%** in these areas respectively.

Figure 5: Biggest barriers to IoT implementation



The IoT introduces a wide range of new security risks and challenges to devices, platforms and operating systems, their communications and even the systems to which they're connected (such as using IoT devices as an attack entry point).

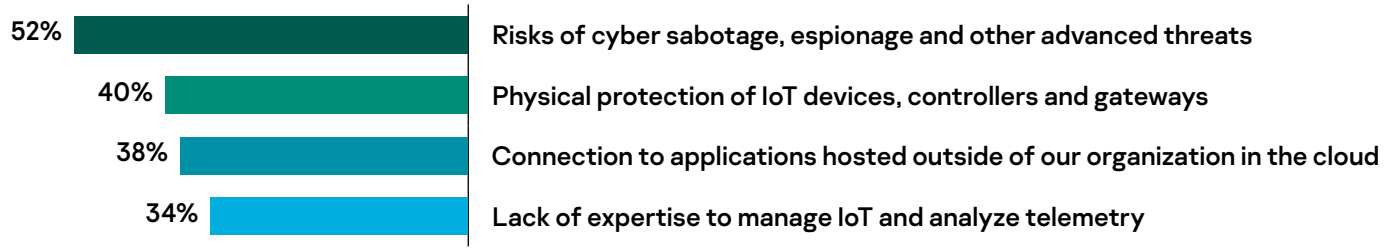
When we asked organizations about their specific concerns, we found they are particularly worried about collecting big data from IoT devices as they perceive risks of cyber-sabotage, espionage and other advanced threats (**52%**).

IoT projects are very fragmented, loosely-coupled, domain-specific and integration-heavy in nature. In comparison, IT projects such as messaging/communication, analytics, CRM, etc., have around 80% of common requirements. In the case of IoT implementation, however, we have to deal with all kinds of legacy systems, physical constraints, domain protocols, multiple vendor solutions, etc., and maintain a reasonable balance in availability, scalability and security. In pursuit of higher availability and scalability, certain cloud infrastructure has to be leveraged, the system has to be open to some extent, then security becomes an enormous challenge," comments Eric Kao, Director, WISE-Edge+ of Advantech, a global vendor of industrial IoT solutions.

"The pandemic simply exacerbates the whole situation. Employees have to work remotely connecting to production systems, opening up even more vulnerabilities. Key applications and infrastructure have zero tolerance for downtime, which leaves little choice for enterprises and organizations but to pay a huge ransom right away once they are compromised.

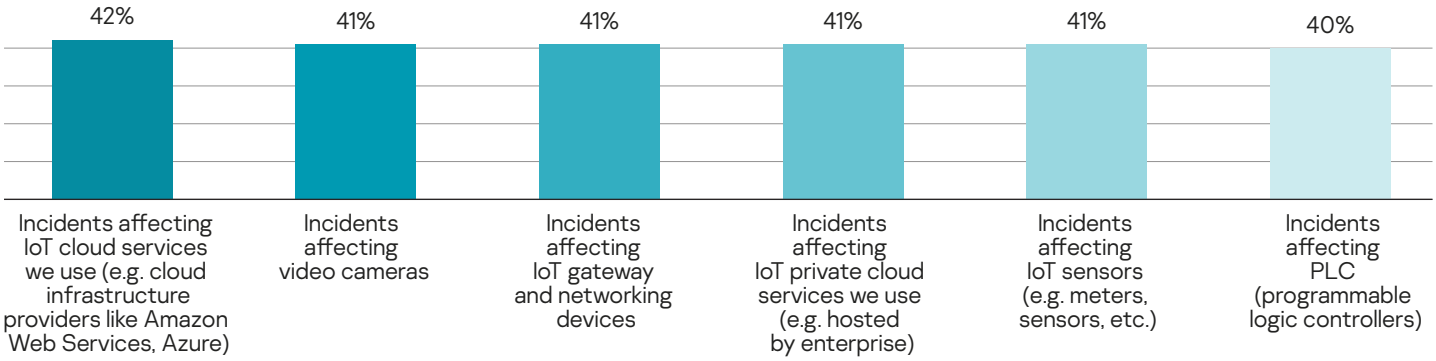
The ransomware attack on Colonial Pipeline is an example of the national-security level of an incident that took place in the US last year. The Pipeline was shut down. It was reported that 75 bitcoins were paid (USD $5M) within hours in exchange for a decryption tool, which proved to be so slow that Colonial needed to bring the system back from its own backup," Eric Kao adds.

Figure 6: Key concerns for big data in IoT



42% of organizations reported being impacted by cybersecurity incidents affecting IoT cloud services (public clouds infrastructure), while **41%** cited incidents affecting IoT gateway and network devices..

Figure 7: Prevalence of attacks on IoT across business areas



Stephen Mellor, Chief Technology Officer at the Industry IoT Consortium (IIC) underlines that organizations can face different issues depending on their profile and the systems they use. But the top issues in decreasing order of importance are:

"Organizational change. Large industrial organizations tend to make long-term bets (the Airbus A380 has still not paid off after 19 years). IoT requires quick action to see what works and what doesn't; what gives value and what doesn't. Also, IT and OT tend to be siloed, with different terms and vocabularies. They also place different emphasizes. IT tends to think first of (cyber)security and OT people tend to think first of safety. Reconciling them is a challenge.

Managing risk. IoT is not simply a matter of connecting your system to the internet. The consequences can be too great. Understanding that risk — and managing it — is key to success. Apart from the threat of hackers, there's also the risk that something might go wrong. Is the 0.5% risk that the factory could be down for two weeks worth the promised 5% improvement in productivity?

Talent. IoT is new and there are not enough experts in integration engineering, analytics, trustworthiness, AI and cybersecurity to be found. Moreover, you may not even know what talent you need. I know enough to stay clear of hardware (and to find an expert to help), but I know enough about AI to be dangerous. We can't know what we don't know, except at the periphery."

Protecting IoT and systems with the highest cybersecurity demands

The good news is that our research found 43% of businesses have some form of IoT cybersecurity measures in place. However, an equal number (43%) of the businesses reported having at least one type of IoT that was not protected.

Organizations face several challenges when protecting IoT. The sheer scale and variety of devices, operating systems, software, and hardware components make it difficult to secure IoT platforms from potential data breaches and attacks on the whole network.

In 2021, **experts at Israeli company JSOF** discovered 19 zero-day vulnerabilities, some critical, affecting hundreds of millions of IoT devices. These vulnerabilities — named Ripple20 — were found in the TCP/IP library of Treck Inc., which JSOF has been developing for more than two decades. The library is present in a wide range of IoT solutions, affecting items from home and office printers to industrial and medical equipment.

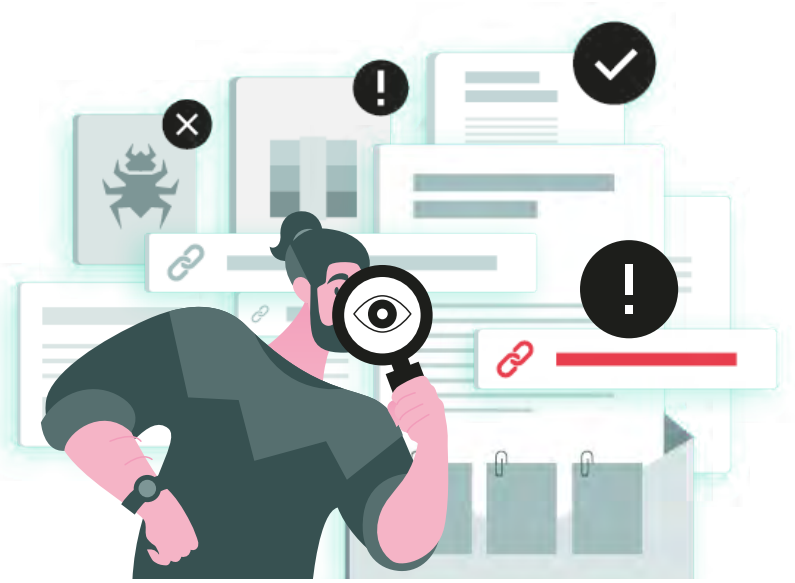
Unlike hardware and software for PCs or mobiles which are well researched and standardized, it is impossible to study all IoT devices and ensure the reliability of conditions for their development, making errors, vulnerabilities and undeclared functions inevitable.

Another setback is that there are many open-source software platforms for IoT development. These components are often not tested for cybersecurity, so vulnerabilities can find their way into the developed product and persist for many versions. One example of this would be a 'zero-day' attack, which takes place when hackers or malicious actors exploit the flaw before developers have a chance to address it. These types of attacks are especially dangerous because once criminals have infiltrated a network, they can either attack immediately or sit and wait for the most advantageous time to do so.

But using a standard endpoint anti-malware protection solution is not the way out of this problem. Moreover, there are some devices on which anti-malware solutions cannot be installed due to insufficient performance or resources.

A further challenge for businesses is the difficulty of rolling out updates to IoT devices and platforms. Unlike the more versatile PCs and mobile devices, for which IT departments usually have effective tools for timely updates, IoT solutions can consist of many different applications, systems and pieces of software with no single approach to updating and patching. Updating such systems is a laborious and not always feasible task.

> "Cybersecurity must be front and center for IoT. Managing risk is a major concern as life, limb and the environment are at stake. An IT error can be embarrassing and expensive; an IoT error can be fatal. But cybersecurity is only one part of making a system trustworthy. We need also physical security, privacy, resilience, reliability and safety. And these need to be reconciled: what can make a building secure (locked doors for example) could make it unsafe if you cannot get out quickly," adds Stephen Mellor.



The call for Cyber Immunity

In order to respond to IoT security challenges and provide help to companies requiring specific cybersecurity protection, activities on different levels must emerge.

There is movement towards standardizing the development and implementation of IoT platforms to make them more reliable and secure. Such initiatives are born in associations like The Institute of Electrical and Electronics Engineers (IEEE), The International Telecommunication Union (ITU), The European Telecommunications Standards Institute (ETSI) and so on. National-level policies that require specific cybersecurity measures from local players have already begun being implemented.

There are also recommendations for businesses on how to approach building secure IoT systems or how to assess the state of IoT solutions already in place, such as one from Industry IoT Consortium — "IoT Security Maturity Model". It guides organizations through processes that will help them adopt sufficient security measures for specific cases.

Common recommendations for IoT security involve using encryption and strict password policies, vulnerability management, network segmentation and Zero Trust model, as well as firewalls and dedicated protection for cloud infrastructures with which IoT devices connect. These practices are essential for all critical operational technology systems.

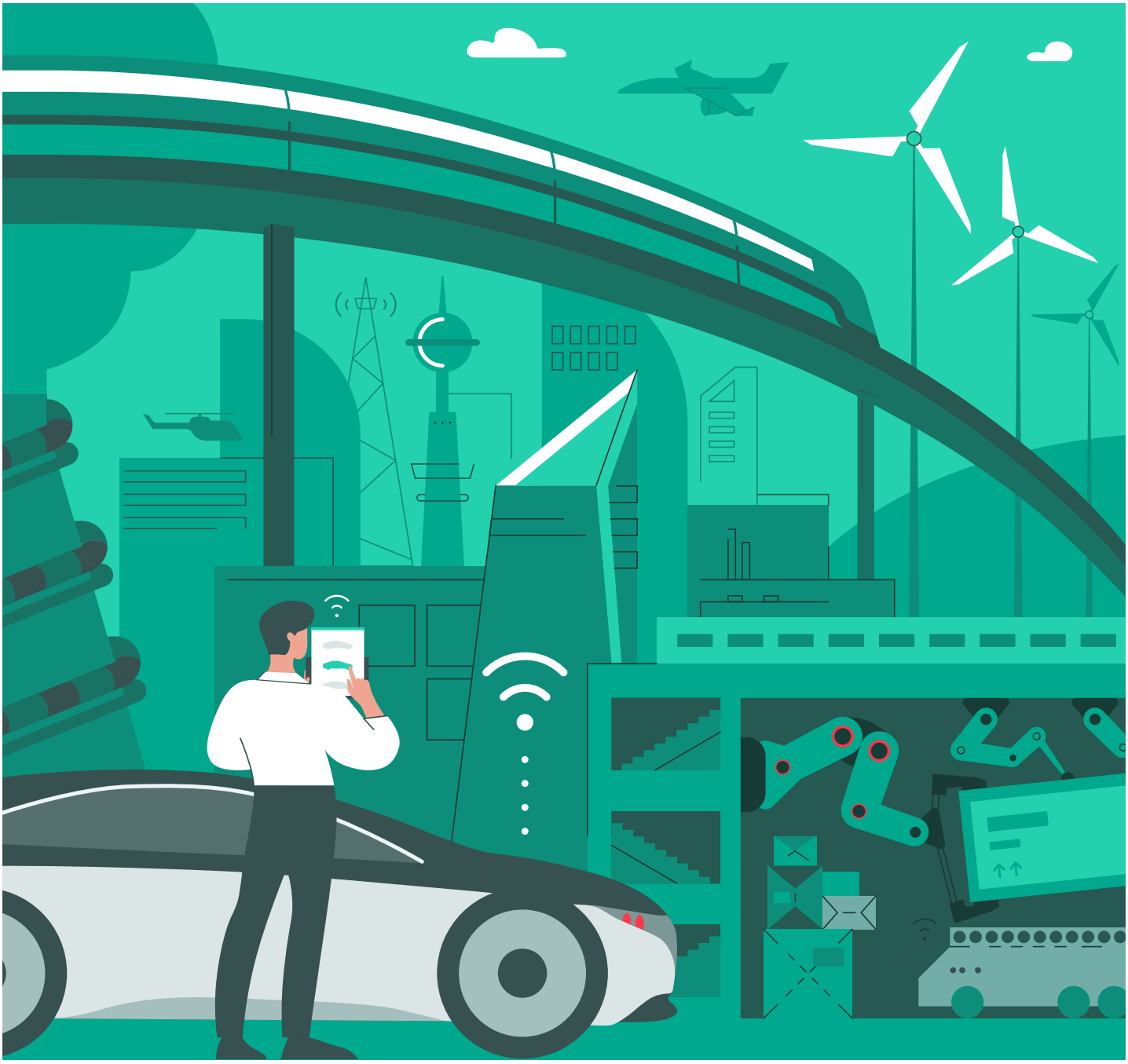
Stephen Mellor also suggests that, "prediction is difficult, especially about the future", as a baseball player once said[1]. But it seems clear that there will be advances in:

- Zero-trust security. This is the idea that you assume that everything is a threat and only accept communications once you have been convinced that the other party is safe.
- Assurance cases. These are statements that represent the state of security of a component. They have been in use for some time, but we can expect further formalization.
- Security by design. An approach that formalizes infrastructure design and automates security controls so that you can build security into every part of the system development process and the eventual system.
- Software bill of materials (SBOM). This is a description of all the software, including versions and included sub-components, that make up a given component. This is necessary to guarantee assurance and to be able to identify components with flaws when a threat emerges.
- Artificial intelligence. AI will be used increasingly to identify threats and automatically address them.
- And how better to finish than with quantum cryptography? Quantum computing can crack passwords far more rapidly than traditional computers. We need ways to distribute keys so that we can know that no one has looked at them. Quantum cryptography (more properly, quantum key distribution) makes this possible because measuring a quantum system disturbs it and can therefore be detected."

1 The phrase is believed to be attributed to Yogi Berra

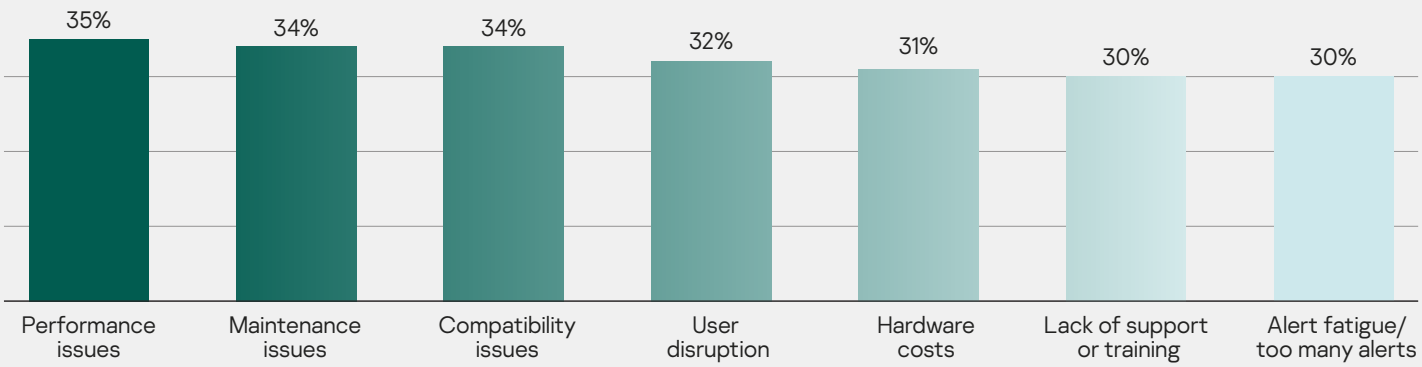
Additionally, there is a specific approach to IoT security, called **Cyber Immunity**, that is necessary when protection is an innate function of the IoT platform. Cyber Immunity is focused, not on reducing the number of potential vulnerabilities, but on creating conditions where the exploitation of vulnerabilities does not affect the basic functions of the overall system. Therefore, even if an application is compromised, it will not affect the operation of the entire platform.

This can be achieved with a specific operating system and methodology for platform development. This operating system uses a microkernel architecture, with only a few thousand lines of code, which minimizes the risk of vulnerabilities and reduces the attack surface. This structure, using minimal number of trusted components in the OS, along with security domain isolation, scanning of interprocess communications and MILS architecture (Multiple Independent Levels of Security), ensures that most types of attacks are unable to affect the system's functions. These principles are utilized in **KasperskyOS**, which can be used in IoT, smart cities and other connected systems.

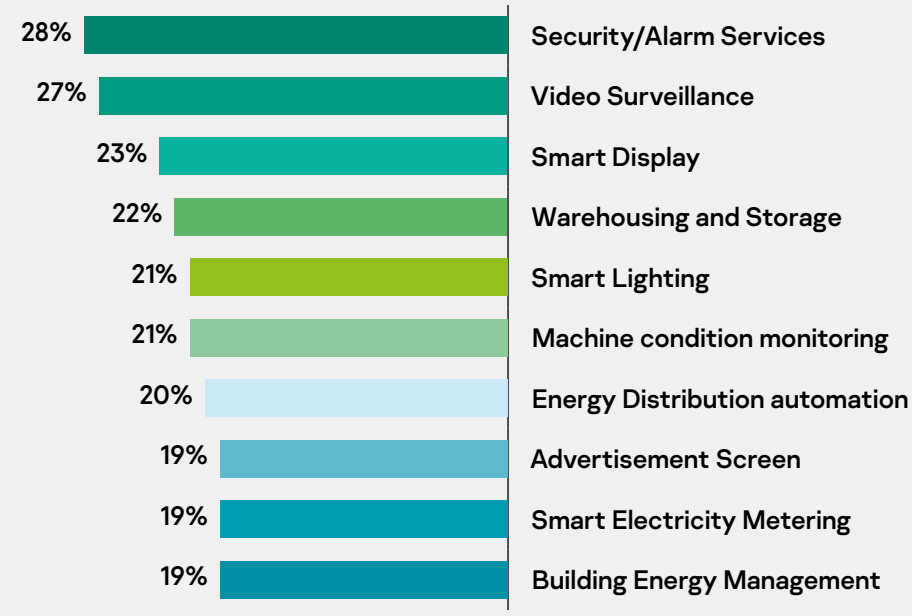


Appendix:

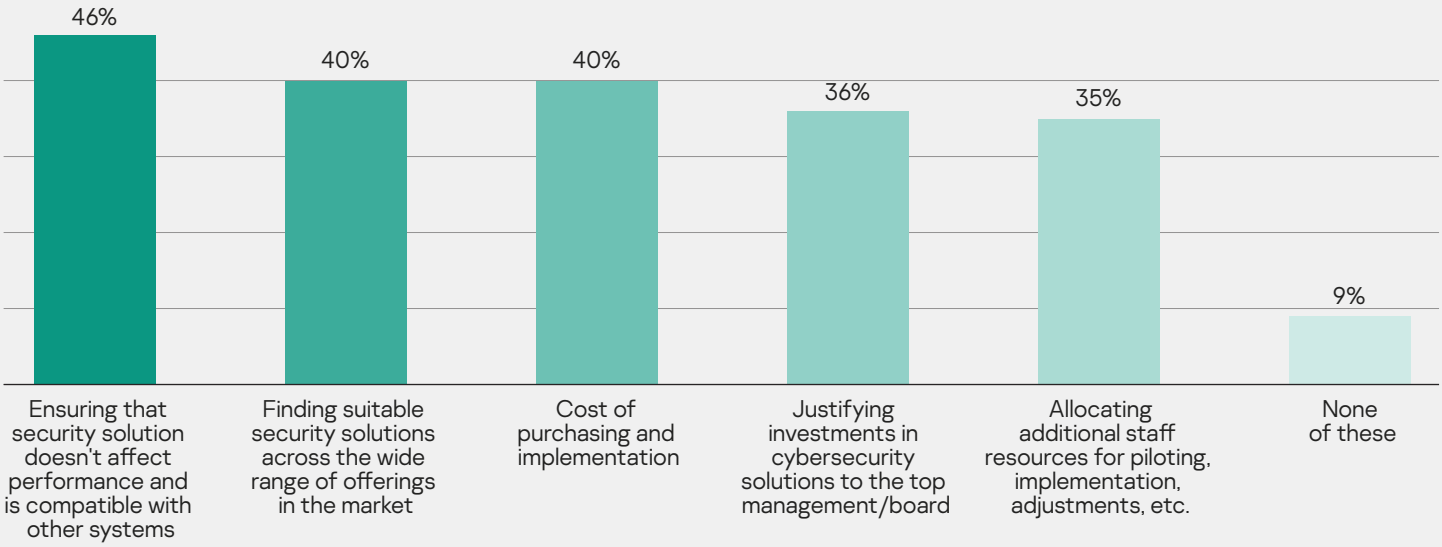
Top issues with cybersecurity solutions organizations face



Types of IoT seeing the widest reported growth (% business reporting increased use)



Top issues with cybersecurity solutions organizations face



Cyberthreat news: securelist.com
IT security news: business.kaspersky.com

kaspersky.com

kaspersky

GBD-8963 Q1/22 V1