BI.ZONE

The path to digital leadership

A practical guide on incident management

"

Cybersecurity
is one of the foundations
of business sustainability
and continuity in the future,
and it is becoming an important
part of every organisation's
brand and reputation.
In this era and in the future,
it will be the foundation
for reliable technologies
and businesses.

Klaus Schwab,
Founder and Executive Chairman,
World Economic Forum

Introduction

A year ago, during the pandemic, companies were worried about moving to remote operations: many were simply not equipped or ready for the transition.

Today, the online workplace is no longer an intimidating concept. It has become clear that digitalisation ensures competitiveness.

In this climate, it is essential to maintain stable processes that are resilient to cyber incidents.

This guide provides real examples of the challenges that companies may face and ways to overcome these challenges in the digital space with the least impact on business functions.

The content is divided into three independent sections, which can be approached in any order depending on the challenges you are currently facing.

Each section is prefaced with its key points, followed by a conclusion at the end, so you can quickly understand the essence.

This material is strictly educational to help you understand the basics of incident response. This is not an official standard, but it will make it easier to navigate the topic.

In addition to our recommendations, it is important to also consider global best practices compiled in the following documents.

Cybersecurity incident response standards

- ISO/IEC 27035:2016 — Information technology — Security techniques — Information security incident management.
- NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide.
- SANS Incident Handler's Handbook.

Business continuity management standards

- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.
- ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA).
- ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.

Business in the digital age: threats and opportunities

Key trends

The main competitive edge for companies today is how well they adapt to the digital environment. This environment dictates that we focus on the stability and resilience of our infrastructure.

Here are 5 safe digital transformation trends that are definitely worth looking into.

01 Secure remote workplace

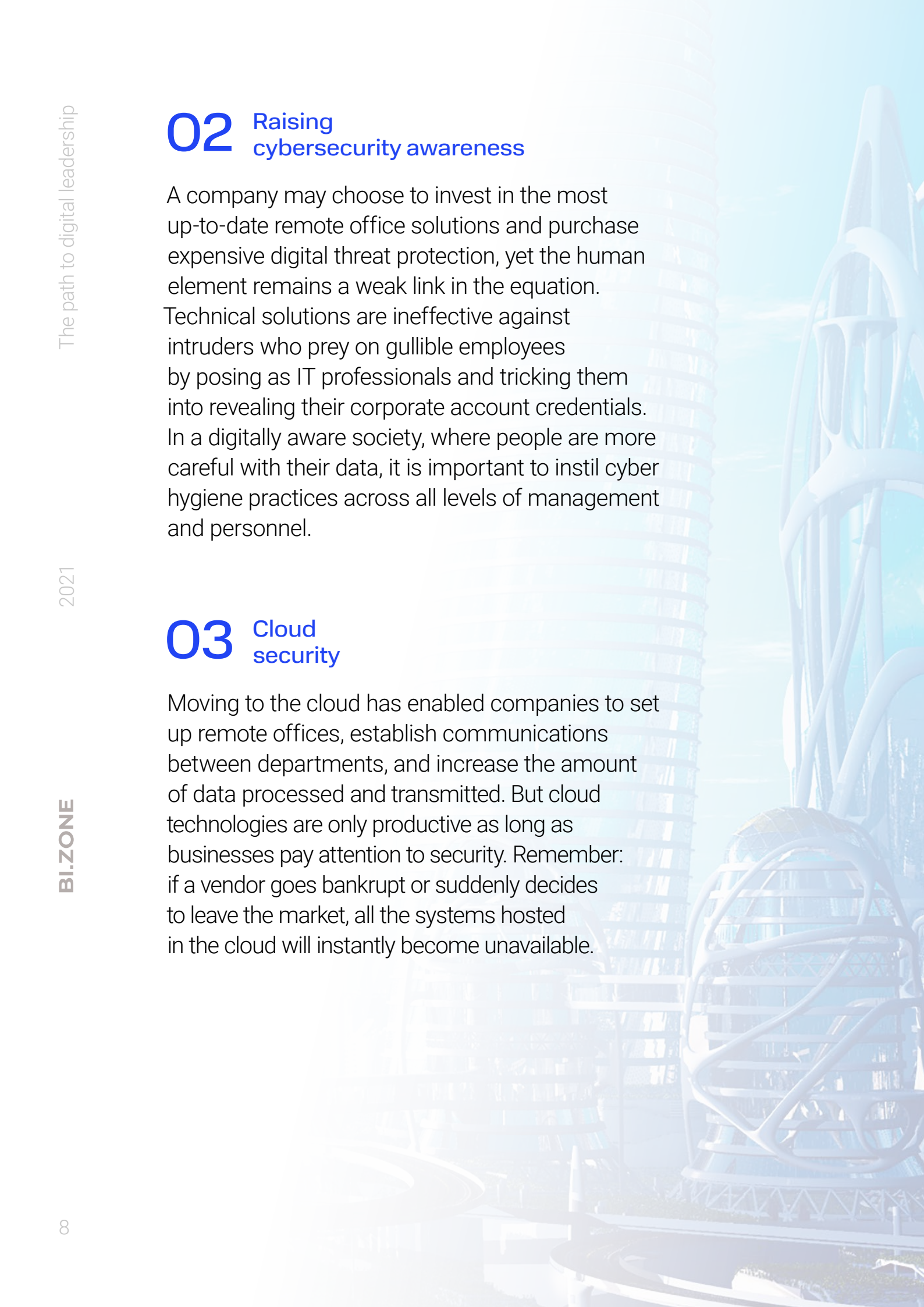
The more remote connections to the corporate network, the greater the risks of overloading it and causing downtime. It also becomes more difficult to keep track of digital assets and look for potentially vulnerable ones that could be used as an entry point to the company network. Finally, a coffee spill on a laptop will interrupt work indefinitely, as the employee will not be able to quickly run to the IT department and ask for a replacement. Even such trivial accidents require an effective action plan.

02 Raising cybersecurity awareness

A company may choose to invest in the most up-to-date remote office solutions and purchase expensive digital threat protection, yet the human element remains a weak link in the equation. Technical solutions are ineffective against intruders who prey on gullible employees by posing as IT professionals and tricking them into revealing their corporate account credentials. In a digitally aware society, where people are more careful with their data, it is important to instil cyber hygiene practices across all levels of management and personnel.

03 Cloud security

Moving to the cloud has enabled companies to set up remote offices, establish communications between departments, and increase the amount of data processed and transmitted. But cloud technologies are only productive as long as businesses pay attention to security. Remember: if a vendor goes bankrupt or suddenly decides to leave the market, all the systems hosted in the cloud will instantly become unavailable.



04 New approaches to cybersecurity incident management

The distinction between cyber and business risks has somewhat vanished: modern digital threats can cause just as much damage as office fires. Addressing business risks is a complex and multifaceted task that involves different departments – cybersecurity, IT, PR and others, depending on how the organisation's processes are structured.

05 Outsourcing secure digital transformation

Experts are in short supply these days, and it may be difficult to find staff capable of building reliable infrastructure. However, it is even more difficult to maintain a working infrastructure and make it resilient to disasters. Some digital transformation tasks simply require too much labour and expenses. As a result, companies are becoming more open to the idea of outsourcing secure digital transformation and business continuity management. External experts help companies reduce the cost of digitalisation and address staff shortages.

The pandemic has triggered a digital revolution and changed the world of business: IT and retail are no longer the only driving force for moving operations online, now healthcare providers, commodities companies and government agencies are also making this strategic transition.

In Russia, state-owned companies alone managed to achieve a 54% digitalisation rate in the year 2020[1]. The government has many plans to develop this trend: to ensure digital maturity of public administration and key sectors of the economy and the social sphere, to quadruple the amount of investment in Russian IT solutions, and to increase the volumes of social services provided electronically to 95%. Progress in this direction is already visible today: online social service features enable users to register a transaction, file a tax declaration, and check fines.

The World Economic Forum believes that the always-on connectivity principle has become integral to our everyday lives[2]. This also affects corporate processes: companies want to continuously communicate with the public and instantly respond to any changes.

54%

average rate of digitalisation among Russian state companies in 2020[1]

1. Digital transformation in Russia: 2020 results and development outlook // Analytical Center for the Government of the Russian Federation
2. Technology futures: projecting the possible, navigating what's next. Insight Report April 2021 // World Economic Forum

In this environment, there is a growing need for businesses to build robust and cyber-resilient business systems that are able to defend against digital threats in real time. International Data Corporation (IDC) estimates that organisations spent $125.2 billion on cybersecurity products and services in 2020, up 6% from 2019[3]. As the global economy recovers from the COVID-19 pandemic, IDC predicts spending will rise to $174.7 billion as early as 2024, with an average annual growth rate of 8.1% for the 2020-2024 forecast period.

But mindless investments are not going to get the job done – the building of a robust and cyber-resilient system requires a calculated approach.

Based on our project experience and analytics, we've identified 5 trends for secure digitalisation. These trends will help you focus on the essentials of strategic security and make your business more competitive in the digital age.

We highlight current trends using data on the levels of digital maturity of companies across various economic sectors.

BI.ZONE started this research in 2018 with new conclusions released annually. The research examines over 150 companies from medicine, media and e-commerce, transportation, finance, retail, telecommunications and IT[4].

A company's maturity level is assessed and given a score of 0 to 5, where 5 means that a certain function or expertise in the company is well developed, and the company works consistently to improve its cyber resilience, and 0 means that the function is not developed at all.

3. Ongoing demand will drive solid growth for security products and services, according to new IDC spending guide // IDC
4. Threat Zone 2020: Not waiting for thunder // BI.ZONE

Secure remote workforce

The main trend set at the start of the pandemic, and still relevant today, is the drive for companies to maintain business continuity while working remotely.

Too many connections to the corporate network lead to a collapse in the network due to excessive traffic. The company stops functioning, leading to huge costs and unforeseen expenses to get operations back up and running. In some cases, such a crash could be critical. For example, if a corporate gateway stops responding to network connections, you risk missing important emails or online meetings with partners.

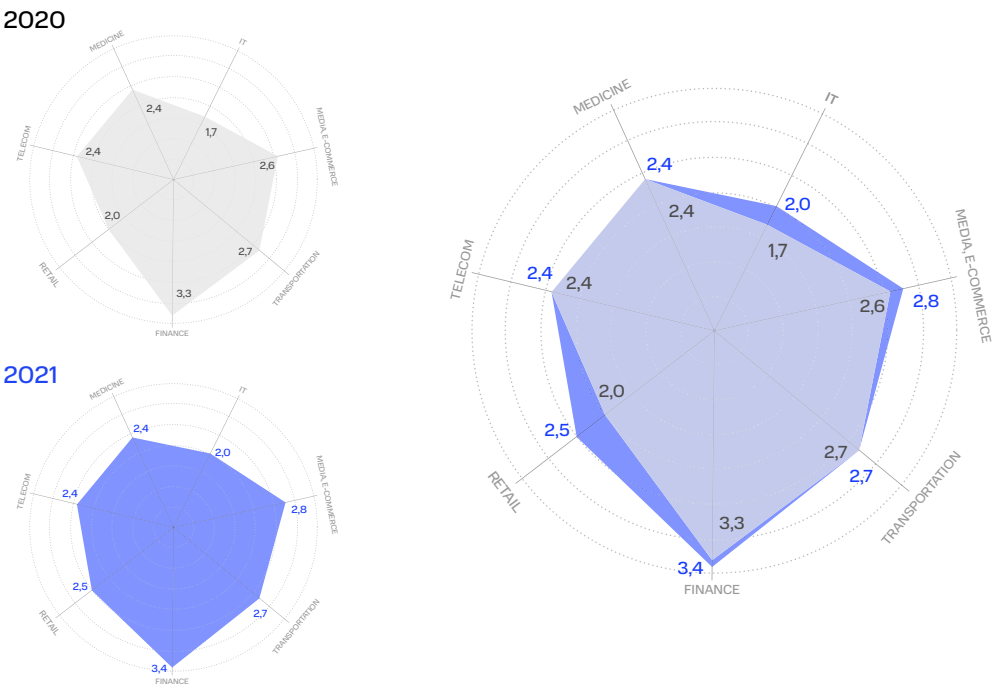
35%

of companies took extra measures to protect their remote access in 2020

Cybersecurity services are finding it harder to secure the remote workstations for employees and protect the data in transmission channels. As a result, companies are facing new digital risks that come with greater consequences for the business. For instance, malware may infect a corporate network and shut down the electronic document management system. This may prevent the company from shipping goods and thus lead to losses in the form of lost profits and fines. Several years ago, this happened to Moller-Maersk, the world's largest shipping operator: the company lost $200 to $300 million following a ransomware attack[5].

Thus, a secure remote workforce has become one of the elements of a stable infrastructure.

System access control



5. Mimoso M. Shipping Reports $300M Loss Stemming from NotPetya Attack // ThreatPost

Minimising the risks and ensuring continuity of a remote workplace begins with controlling access to information systems. In the past year, 35% of organisations have taken additional steps to protect remote access. While it is true that companies across all industries are taking a more responsible approach, the financial sector is still leading the way for the second year in a row.

The first step to securing your telecommuters is to control access to company information systems and to protect employees' personal and corporate devices. You have to remember that your employees may choose to connect to the corporate network via their home router with a default password, or through an unprotected hotspot on the train. These "invisible users" put your corporate infrastructure at risk.

Make sure to use a VPN, build up your security tools and always update your software on time. This process can be optimised by developing organisational measures which would include security policies and briefings.

Beware of service unavailability and downtime from heavy network traffic and increased user connections. An inventory of your digital assets (computers, servers and other information processing devices) can help you avoid these problems.
Also, routinely evaluate the capacity you need to keep your remote office running, especially at peak times when everyone is actively connecting to company resources, reading emails, viewing documents in the cloud, etc.

Raising security awareness

Cyber hygiene is just as important as personal hygiene, which is why people and organisations are concerned about creating a secure information environment.

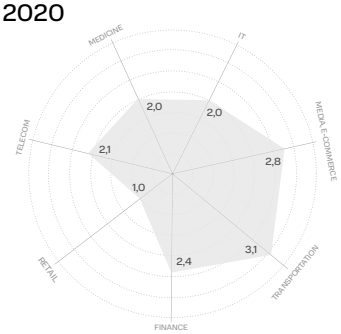
The human element affects business continuity as much as technical equipment: an error can lead to interruptions, accidents or even cyberattacks. You can buy all the advanced solutions and build up a robust defence, but if employees fail to recognise phishing emails or malicious software, such investments will not pay off.

68%

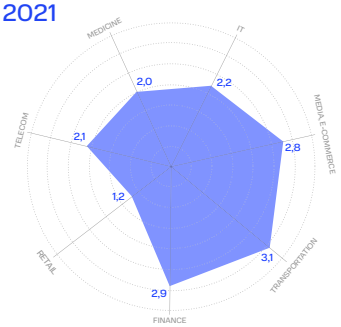
of sales representatives fall for online fraud

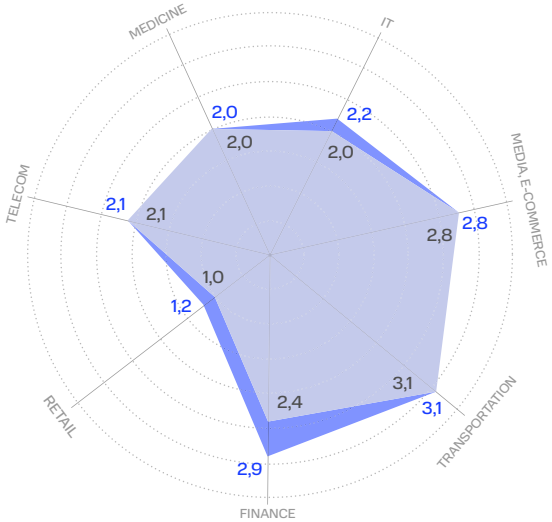
Cybersecurity awareness trends

2020



2021





Company employees are now a very lucrative attack vector because they are simply not used to maintaining good digital hygiene. The phishing attacks we have simulated on our clients as part of a training exercise reveal that 7 out of 10 sales representatives will fall for the tricks used by cybercriminals.

Most of the organisations included in the research have either already implemented an awareness raising programme or have plans to do so. However, many organisations still lack a clear understanding of how to build an ongoing learning process that covers digital hygiene and safe online conduct.

Reduce human error by promoting a strong corporate digital culture and the basics of cyber hygiene. Here's how to do it.

Take advantage of cybersecurity services, courses and trainings to equip your staff with the skills to avoid being tricked by cybercriminals. Make sure the training is delivered to all levels of staff: senior management, department heads, general employees.

Companies that have already taken the first steps in this direction should focus on a systematic approach to training. Try different methods: introduce regular webinars, publish a newsletter with guidance from cybersecurity experts.

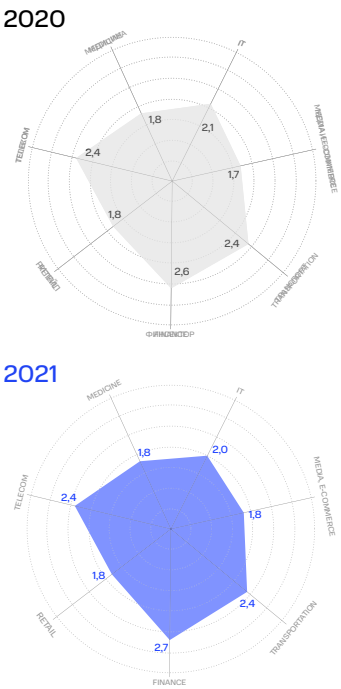
One way to stay in shape is to conduct occasional training attacks which simulate real situations. This task is best outsourced to external experts who will model the attack, collect analytics and provide recommendations on how to make your crew more resilient to digital threats. Security awareness solutions can be used to address all of the above challenges.

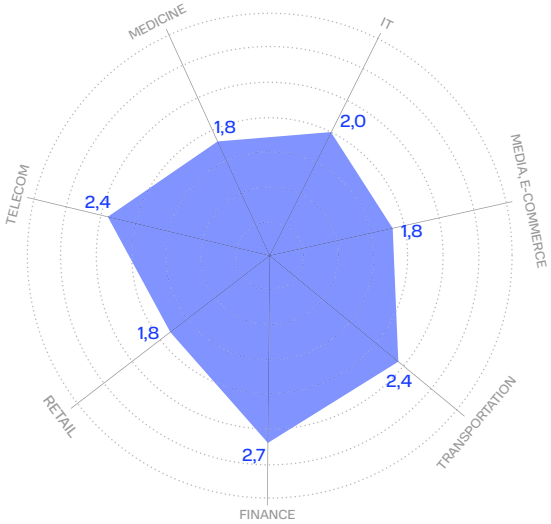
Cloud security

The pandemic has led many executives to consider moving their business systems to the cloud, i.e. to a provider responsible for keeping those systems up and running. The need for this transition has been felt by both small companies and large corporations alike.

In the case of small and medium-sized business, this technology helps companies focus on core business processes and not worry about digitalisation, switching to online, setting up communications, providing access to the network.

Security of communication and relations with third parties





Larger companies use the cloud to back up information, ensure the resilience of their IT infrastructure, and test their business continuity plan.

When talking about the cloud, it is worth mentioning the security of communications. This is one of the most important areas of business security in the digital environment, but many companies overlook it, focusing only on protecting data within their own perimeter. At least 15% of organisations in our research used public storage for file sharing without additional security tools. Also, about a third of the companies do not insist on an NDA with their counterparties and sign it only at the request of the other party. This can easily lead to data leaks from publicly available channels.

The mass adoption of cloud technologies led to companies experiencing new challenges, the biggest one being that company services are now outside the company's control.

Based on our cloud project experience, we would like to point out the risks that go with vendor lock-in and vendor lock-out. This means that organisations are highly dependent on the products and services of a single vendor.

In the case of vendor lock-in, the company becomes hostage to the cloud service provider: it becomes almost impossible to switch vendors. One of the reasons for this is that data may be stored in formats that only the current vendor can process, for example. Dishonest vendors even manipulate the cost of services by taking advantage of customer 'attachment'.

It's not easy for a company facing vendor lock-out, either: if the vendor goes bankrupt or suddenly decides to leave the market, all the systems hosted in the cloud will become suddenly unavailable.

Such was the case involving a steel manufacturer, wherein the company was faced with the same problem when SAP stopped supporting an older version of its software, and a migration to the new one proved to be too costly. As a result, the employees had to quickly convert and learn a new solution[6]. Import substitution helps to avoid such situations.

6. SAP fines Russian steel producers [SAP nakazal rossiyskikh metallurgov] // CNews

If you are going to use cloud services, make sure that the provider has adequate cybersecurity. You can check this yourself using the Cloud Security Alliance approach[7], or you can hire external experts to help you. This will also in part protect you from vendor lock-out.

To protect yourself against vendor lock-in, you have to do some research in advance as to which solutions the vendor uses in their work, what formats they store customer data in, and whether they are compatible with formats of other vendors.

Always insist on the conclusion of an NDA, carefully study the terms of the contract with the provider and always make all necessary corrections.

But remember, although the contract between the customer and the provider often stipulates that the provider ensures data security, the customer is still the owner of the data placed in the cloud. This means that the customer is legally responsible for keeping it safe. However, if confidential information leaks out, financial liability can and should be placed on the provider.

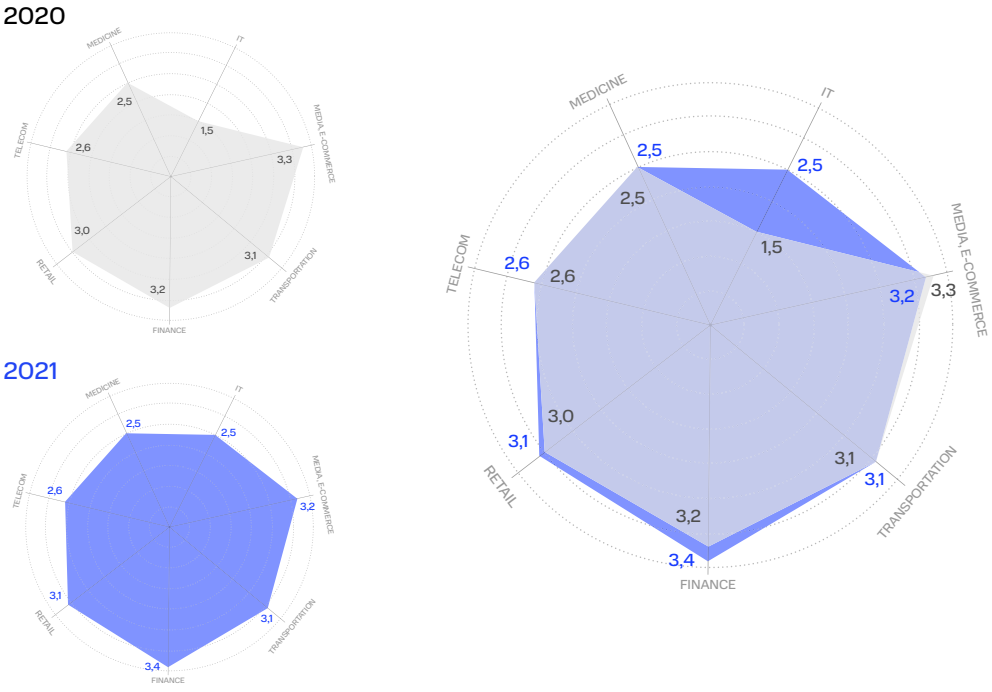
7. Cloud Controls Matrix (CCM) // Cloud Security Alliance

New approaches to cybersecurity incident management

Companies have realised the extent to which incidents in the digital environment can interfere with business continuity. This has sparked two trends:

- to test and implement new approaches to business incident management
- to plan crisis response measures that are effective and not too costly.

Incident management



Business continuity is largely contingent on digital security controls. Today, around 20% of companies still prefer to deal with incidents only when they occur. They lack a clear strategy because they do not see any economic sense in it. Though this is contrasted by the 80% that are actively looking for a more structured and sophisticated approach.

Companies concerned about protection against cyber risks tend to use advanced technologies. For example, they set up Security Operation Centres (SOCs) based on special SIEM (Security Information and Event Management) solutions. These systems are designed to handle a large number of security events from multiple devices, allowing SOC professionals to optimise the response to security incidents and prevent negative aftermath.

Organisations are becoming more interested in detecting threats before they materialise and cause damage to the business. This proactive approach is envisaged in MDR (Managed Detection and Response) services, which Gartner predicts will gradually increase and permeate 50% of companies by 2025[8]. Frost & Sullivan believes that the size of the MDR services market will grow to 1.9 billion dollars by 2024, with an average annual growth rate of 16.4%[9].

Finally, the cybersecurity industry is actively developing what is known as Threat Intelligence (TI). Threat Intelligence enables organisations to investigate the goals, tactics and tools used by cybercriminals. This in-depth analytics helps to build digital defences and better prepare for incidents. Today, threat intelligence is often collected manually without any automation, but we expect this to change in the near future as machine learning and artificial intelligence technologies evolve.

8. Market guide for managed detection and response services // Gartner Research
9. Tan M. Rise of advanced cyber threats spurs demand for managed and response solutions // Frost & Sullivan

Remember that any threat can negatively impact business continuity, undermine the resilience of your IT infrastructure, and hit your finances and reputation. For reference, a leak of a single record from a customer database costs a company $150[10]. But reputation is worth far more. After an incident, it can take years to regain customer trust, during which time a competitor can gain a foothold in the marketplace by ensuring continuity of communication with the public.

Keep in mind that the threat landscape is constantly changing, so conventional response methods no longer work. Also, it is better to prevent an incident in advance than to deal with the consequences. Even if you already have a SOC, consider adopting newer and more effective approaches such as MDR.

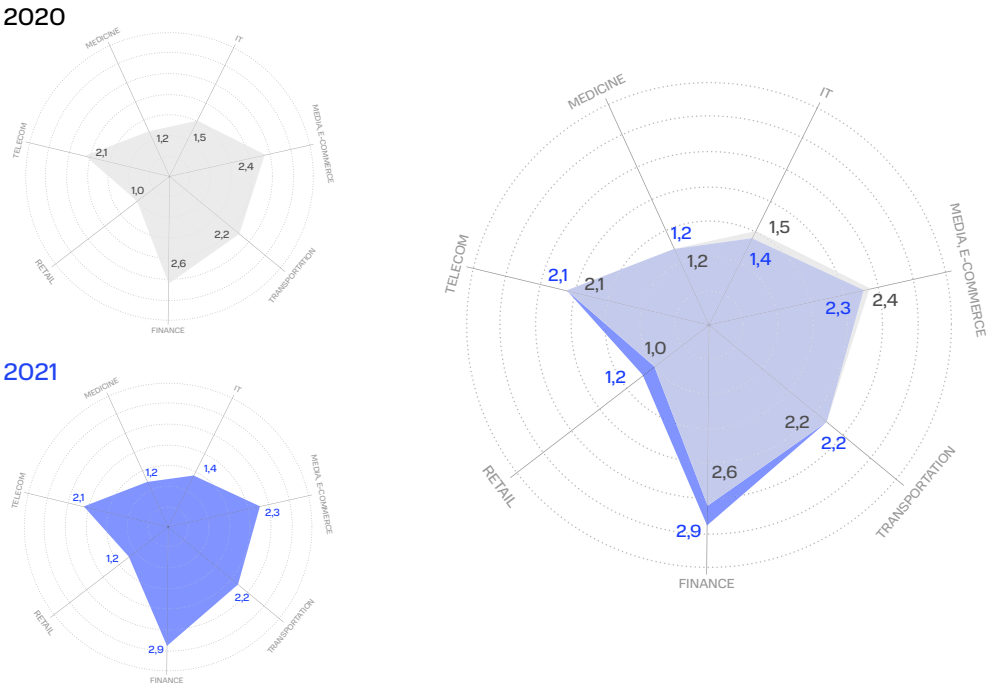
10. Cost of a data breach report 2020 // IBM Security

Outsourcing secure digital transformation

A more calculated approach to IT and cybersecurity has led to the spread of MSS (Managed Security Services) – outsourced cybersecurity management services.

Companies are keen on outsourcing cybersecurity management tasks because it helps them focus on their core business. According to our data, the most notable changes in this direction have occurred in the financial industry and retail.

Cybersecurity management



Three more reasons to choose MSS:

- lower your taxes by not having to purchase expensive protection equipment
- get access to qualified experts, which are currently in high demand
- get professional help from the latest tech solutions on a subscription basis.

International Financial Reporting Standards (IFRS) define expensive data protection equipment as capital assets which are recognised as capital expenditure (CAPEX). The higher the CAPEX, the higher the value of the company's assets and profits. Consequently, there is an increase in income taxes. Under MSS, cybersecurity tools are provided on a subscription basis – this is recognised as an operating cost (OPEX). OPEX reduces the net profit and therefore the company pays less income tax.

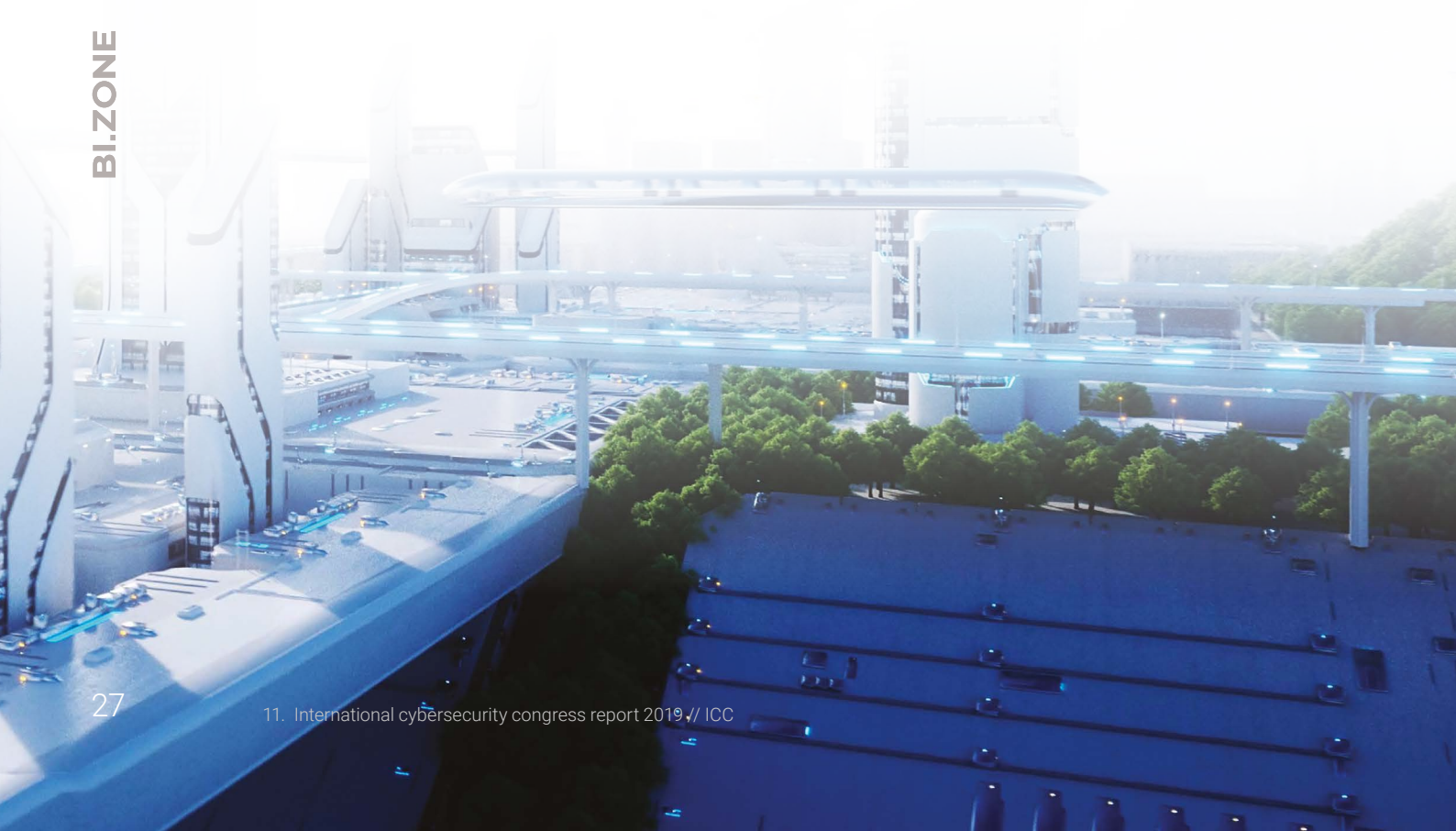
MSS also have a significant effect on reducing costs: according to our estimates, an organisation with up to 500 employees will spend around $600k on building a mature infrastructure, while transferring a portion of the processes to a platform will set the company back $470k. The larger the company, the higher the costs. These figures are based on our experience working with clients and take into account the costs of technical and organisational security measures as well as the salaries for dedicated specialists.

In addition to the capital costs, companies are facing a shortage of qualified personnel: today, the global shortage for cybersecurity specialists sits at 3 million[11]. This situation is unlikely to get any better due to fact that businesses are moving online, so the demand is only going to grow. This is another argument to start looking for a team to help ensure the continuity and resilience of your business in the digital environment.

After all, MSS experts deal with digital security on a daily basis: they continuously monitor trends and provide their clients with the latest technology on a subscription basis. And clients don't have to spend their time researching the solutions market.

save 20%

of your budget by outsourcing cybersecurity functions



11. International cybersecurity congress report 2019 // ICC

Try to calculate the costs and time needed to build a mature infrastructure. Figures can vary depending on the industry, the number of employees, and the current level of expertise. Nevertheless, our experience shows that with MSS you can save up to 20% of your security budget.

Consider business continuity management consultancy services. With the acute shortage of qualified specialists, we expect an increase in demand for the following services:

- BIA (Business Impact Assessment) in a digital environment – investigating how different types of errors can affect business processes
- development of a business continuity plan for digital transformation
- development of a disaster recovery plan after a cyber incident
- creation of a cyber incident management framework that meets industry standards and global best practices.

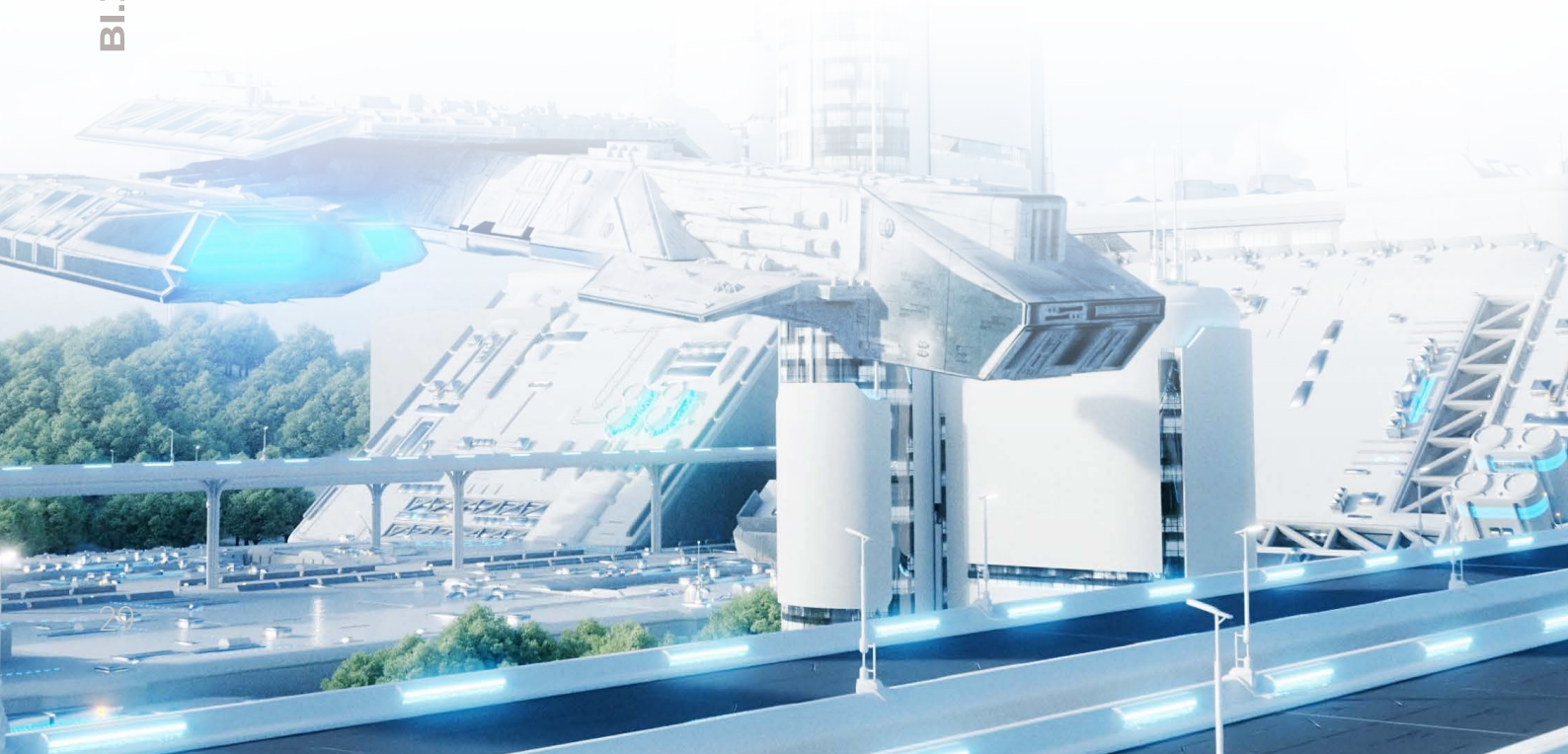
Today, it is still possible to find an expert company that will help with cybersecurity and business continuity management. By outsourcing these tasks, a company can focus on its core business and therefore increase its competitiveness in the digital age.

Conclusion

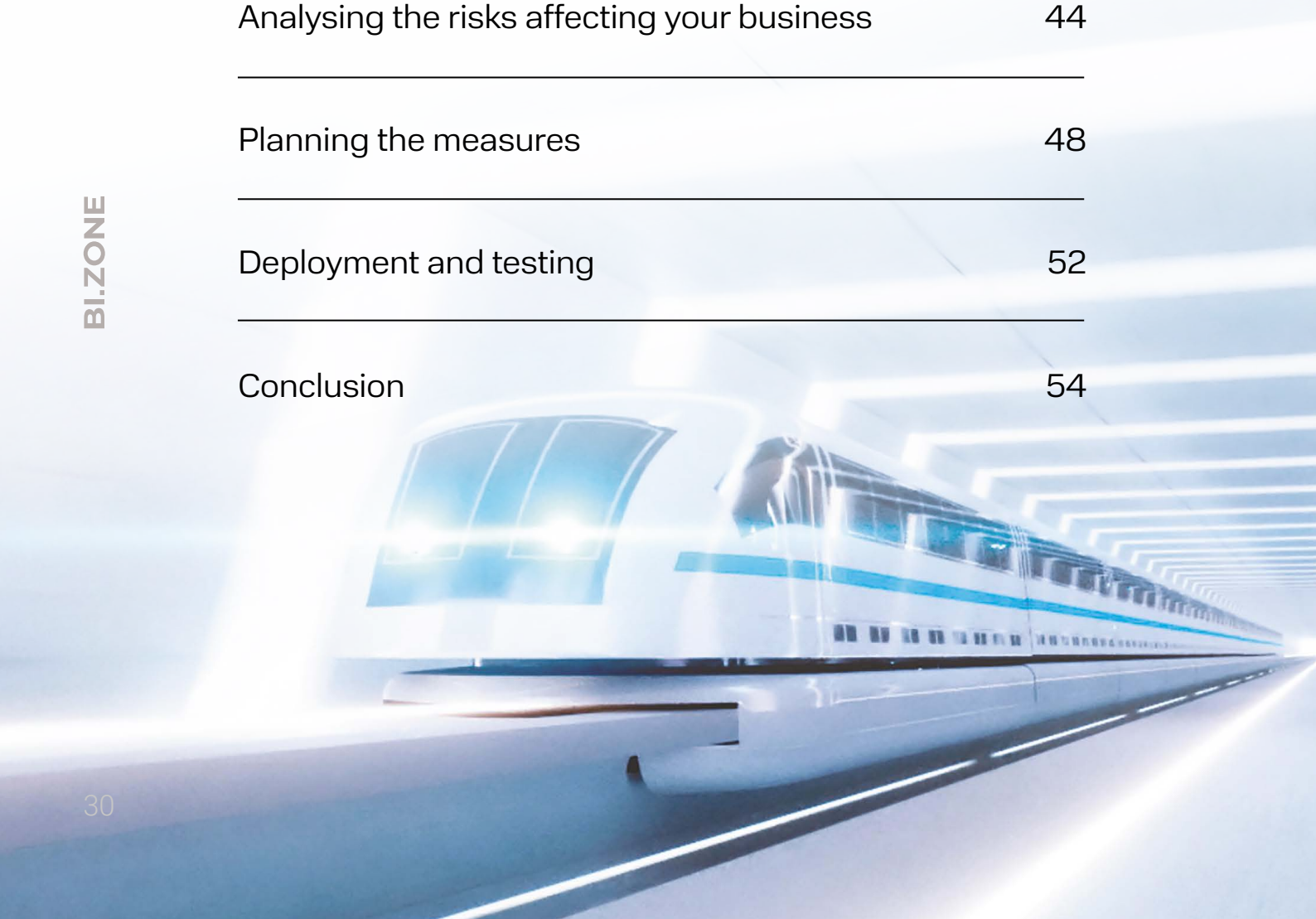
One of the key factors for the success of a company in the marketplace is creating an effective environment for business recovery after an incident. Business continuity management plays a significant role in ensuring sustainable and predictable processes. It helps you to avoid unnecessary costs and maintain an acceptable level of profitability in case of unpredictable events.

It is near impossible to ensure 100% protection against incidents, but you can definitely minimise their impact by having clear response and quick recovery measures in place.

In the next section, we will cover the aspects of ensuring business continuity, building a resilient IT infrastructure, and establishing a business continuity management framework for your company.



Managing business continuity through digital transformation



Key ideas

The faster the pace of digital transformation, the greater is the need for a company to ensure that its business processes run smoothly and consistently. We can refer to business continuity management (BCM) mechanisms to help us meet our needs.

BCM can address a wide range of tasks: online and offline incident prevention, crisis response planning, and disaster recovery. This section will focus on how to achieve streamlined business operations within a digital environment.

The implementation of BCM has several stages that can be divided into two groups: preventive measures and incident response actions. In this part we will look at the process of developing measures in terms of improving corporate cyber resilience. This involves:

- Researching the economic context of business development, analysing the internal and external environment, taking inventory of assets, assessing the market and the geopolitical situation
- Business Impact Analysis – conducting a detailed analysis of digital risks, evaluating all known threats and potential damage to the business
- Planning and developing adequate and cost-effective measures to prevent and respond to business incidents
- Implementing and testing the developed measures.

When researching the external environment, you need to understand the position of your company and your key competitors in the marketplace, you have to investigate industry trends, regulatory standards and other factors affecting your business. All this data will help you better understand the business environment, foresee major changes in legislation, stay aware of competition and be prepared for other factors affecting the company.

When analysing the internal context, you need to compile information about current business processes and take a detailed audit of assets ranking them in terms of importance. Understanding where a major disruption is likely to occur will enable you to develop a number of possible incident scenarios to be prepared for them and ensure business continuity.

Use the Business Impact Analysis to prepare the ground for the implementation of BCM by weighing risks against consequences.

Planning measures involves processing all the information gathered in the first two steps. One of the main mistakes in planning is the formal attitude towards documenting procedures. People are turned off by the bureaucratic language used in guidelines, so instead they rely on informal patterns of behaviour and habits that have been developed over the years. Documents tend to just sit on the shelf gathering dust only to be shown to the auditor once a year. This approach doesn't fit the digital age, where the market is changing quickly, and time is becoming an even more valuable resource. In addition, business continuity is directly dependent on the incident response time, so it is important to start moving away from bureaucracy in favour of simplicity and clarity. Ideally, all documentation should be consolidated into a user-friendly guide that can be referenced at any time.

During the implementation and testing phase, all employees should be made aware of their role in business continuity management. It is important to involve PR, legal, IT and other departments to act as a single unit.

1 in 5 companies

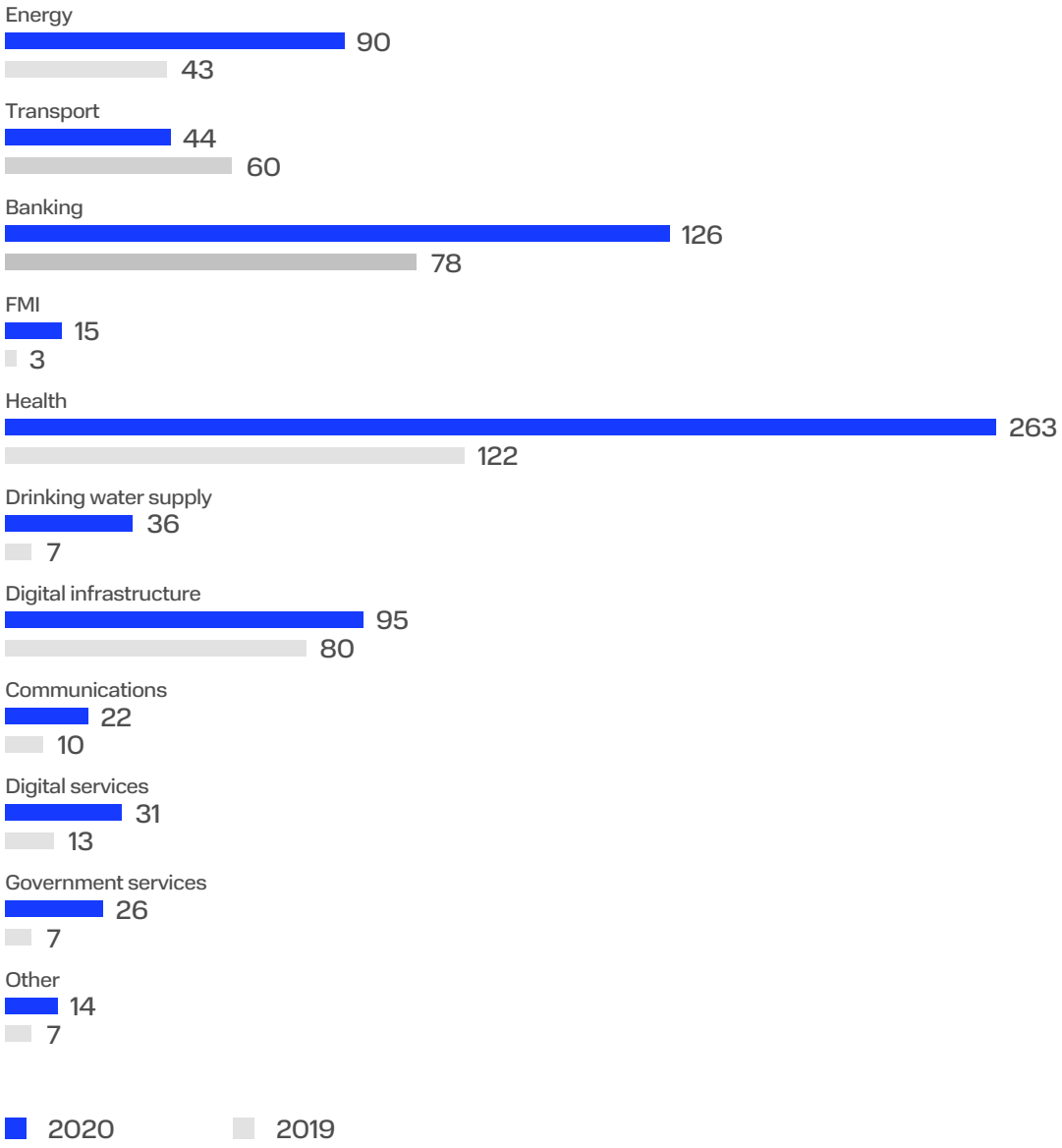
were unable to uphold the same quality of service and maintain continuity of infrastructure during the transition to remote operations

The 5 digitalisation trends from the previous section prove that companies are striving to have a resilient infrastructure, and business continuity management is becoming their first priority.

In this section, we will talk about the basics of business continuity in the digital age and review the key steps for implementing BCM.

> All of our recommendations are based on BI.ZONE's own experience and backed up by our research findings from 2019-2021.

Similar to Section 1, the following comes with materials on assessing the digital maturity of organisations by industry which will help you better understand which direction to go in.

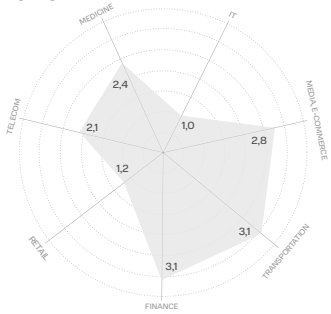


Almost all sectors of the economy have experienced a noticeable growth in incidents in 2019-2020, according to the experts at The European Union Agency for Cybersecurity (ENISA).

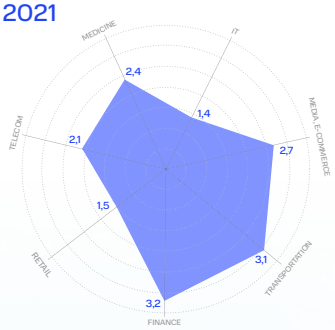
At the heart of BCM is incident management: handling incidents, disaster recovery, and crisis response. What is referred to as incidents means any events that can lead to interruptions in your business processes, loss of control over your production and other dangerous consequences for the company.

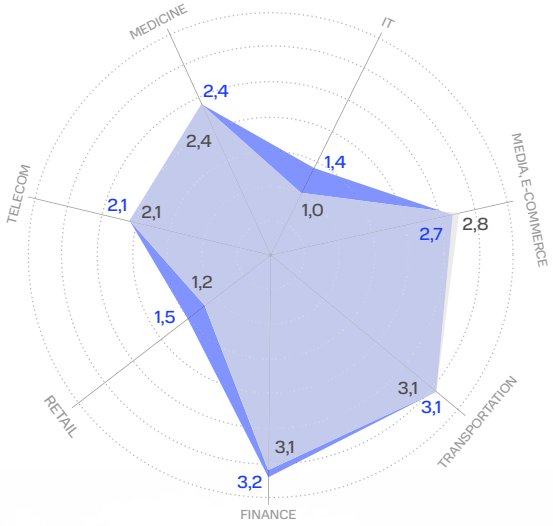
Continuity management

2020



2021





The role of BCM became particularly prominent in 2020, when the world was faced with the pandemic. Not all were prepared: our research showed that 1 in 5 companies failed to maintain service quality at the same level when they moved to remote operations. Many organisations, including those in the digital security sector, saw their business processes lag for a while. The reason for this was the heavy workload on their staff, a lack of time and a lack of necessary technical support. These problems had the greatest impact on companies that had never anticipated possible emergencies and had no set procedures in place to deal with them.

Over the course of the year, organisations adapted to the new situation when some or all of their staff had to work remotely. In business continuity management, improvements are evident in IT and retail, probably due to the industries' increasing reliance on technology and the emergence of new disasters that could disrupt processes. Companies in these industries may have adapted more quickly to the new environment because they were already undergoing an active digital transformation.

The implementation of BCM involves several stages of work:

Development and implementation of BCM tools:

01 Examine the context in which the business is developing: internal and external environment analysis, inventory of assets, market research.

02 Perform a detailed business impact analysis (BIA), which involves assessing threats and potential damage to the business.

03 Start planning cost-effective measures to prevent business incidents and respond accordingly.

04 Implement and test the developed measures.

Response stages in the event of an incident:

01 Incident detection and analysis.

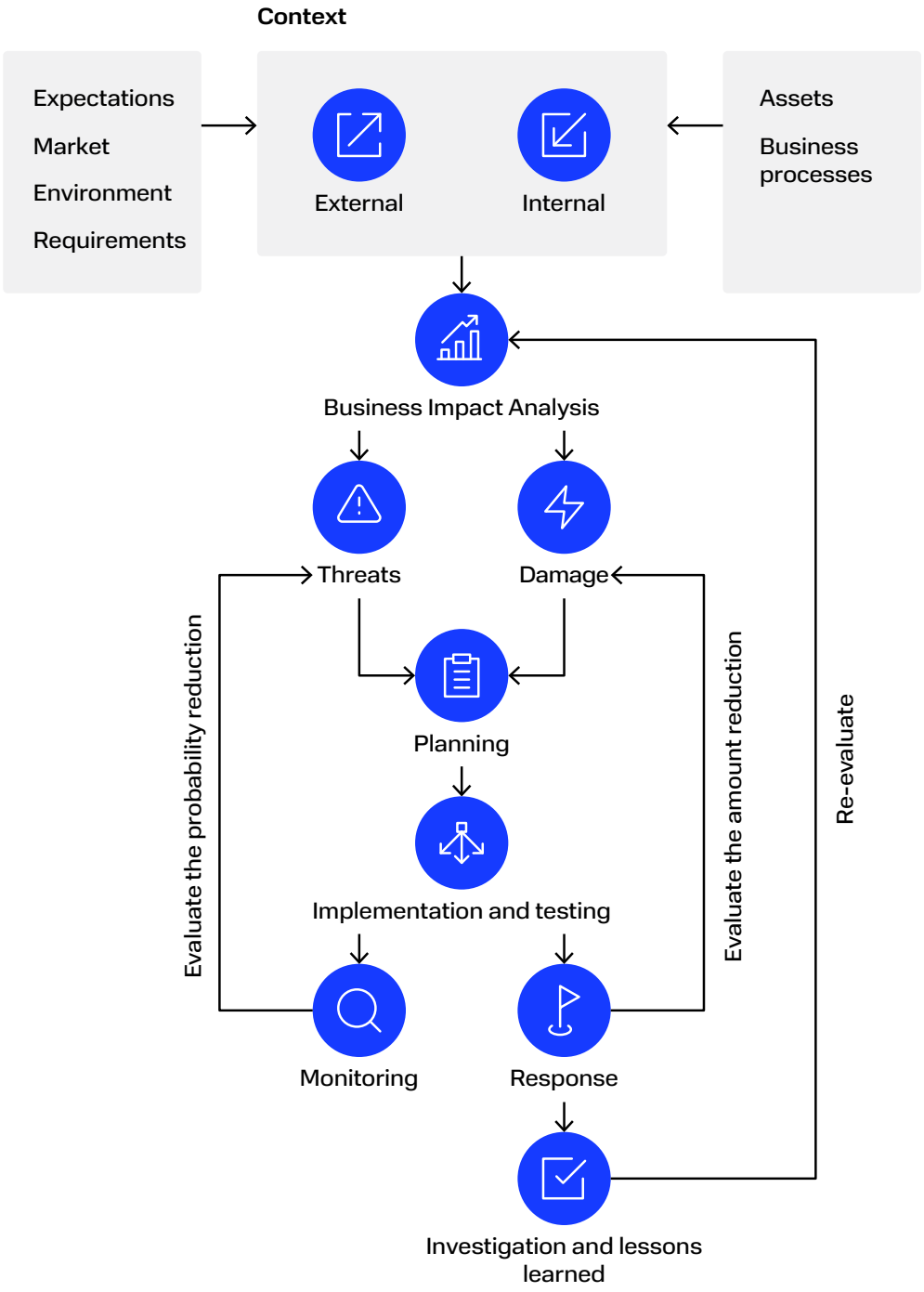
02 Incident containment and process recovery.

03 Root cause analysis of the incident and review of the current tools.

All of this can be seen as a kind of continuity management cycle.

Before exploring each step, we suggest briefing through the detailed BCM diagram.

Our diagram clearly illustrates all the components of BCM and the connections between them. Note that continuity management implies being prepared not only to deflect attacks and deal with the consequences, but also to prevent incidents altogether, to learn lessons and to hone the skills needed for an agile response to any changes.

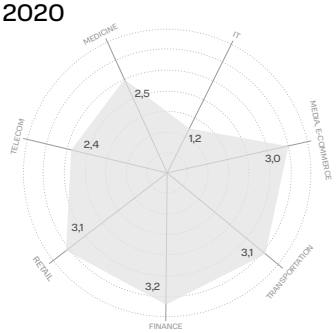


Investigating the company's environment, processes and assets

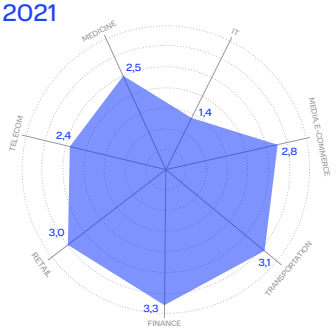
The purpose of the research is to map out the landscape in which the company is developing. This will help you better adapt to the changing market, digital environment and legislation.

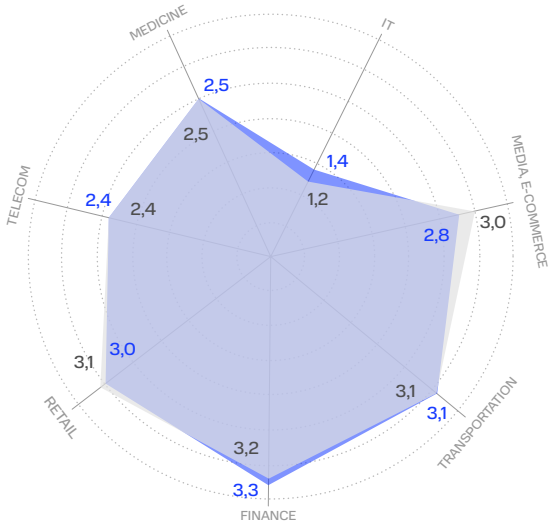
Asset management

2020



2021





When introducing BCM, you must first create a kind of an inbox where you gather information about the current state of the business. For this, you will need:

- external context information: up-to-date analytics on your segment in the market, current regulatory requirements affecting your business
- internal information on current business processes
- information on the company's assets
- an inventory of all the documents that lay out the rules for handling incidents: security policies, response instructions, recovery plans, etc.

Here are the steps to help you successfully manage this phase:

1. Gather all the necessary market information or invite external experts to help you with that. This is done to assess the external environment and to see which disasters impact competitors the most. You may also need to review your marketing strategy in terms of protecting your reputation. Sometimes outsourcing this task can yield even better results through a broader view of the market.
2. Try to visualise the business processes in your company, model the links between departments and define each of their roles.
3. Draw up a list of documents that outline the procedure in case of unforeseen situations. Write up a summary for each of them, also document the rules that exist in your company but are not written anywhere.
4. Take a detailed inventory of assets.

It is advisable to pay a little more attention to asset inventory. This is a basic activity that allows the organisation to:

- identify the most significant resources that need to be protected first
- understand where to direct its budgets when planning for continuity.

It is at this point that serious mistakes are most likely to arise which negate the results of the inventory. Our project experience shows that more than 60% of companies only record assets in terms of financial and business accounting. They fail to keep track of other business-critical assets such as sensitive information, network storage, and projects, all of which are outside of their control. For example, when a company is in the process of switching to remote working, it may overlook a server that handles sensitive information and which would allow easy access to the corporate network.

It is important to remember that a company's level of security is directly related to the completeness and accuracy of the list of network services and web applications on its external perimeter. According to our data, 60% of network leaks and 85% of network compromises are related to undocumented services. These incidents have the potential to disrupt the performance of an organisation and lead to a crisis.

As our research has shown, little has changed in this area over the year. In some industries, the maturity of companies with respect to asset inventory remains low. It may be that companies are not yet used to dealing with the many new types of assets that are emerging in the course of digitalisation. We recommend reviewing your approach to inventory, especially if your company is in a high-risk group.

To avoid all this, you should:

- get a complete inventory of all company assets, including those accessible from the Internet
- evaluate all assets and rank them in order of importance, highlighting those that have the greatest impact on the functioning of the company
- identify the assets that each department works with.

When taking inventory of the digital environment, it is better to use a solution for security monitoring, including the security of the company's Internet-facing assets.

85%

of network compromises involve undocumented digital assets: network services and web applications

Analysing the risks affecting your business

When implementing BCM, refer to BIA[1] for the most effective methods to analyse the impact of risks on business continuity.

The purpose of this analysis is to prepare the ground for implementing BCM: to contrast risks and threats with the consequences to which they may lead. Based on this, you will be able to develop incident scenarios and prepare cost-effective response measures and remediation.

At this stage, you will need to assess and predict:

- the impact of risks on business processes and services
- the possibility of losing particular assets
- external and internal threats to the business
- direct or indirect losses caused by incidents
- unexpected costs for incident remediation
- the impact of various factors on the company's reputation or market position.

1. ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis.

It is advisable to start the analysis as soon as the inventory is completed. Begin by developing a risk profile: identify the threats and vulnerabilities relevant to the most important assets and processes. Involve specialists from different departments: PR can help highlight reputational risks and assess potential damage to the business, lawyers can identify non-compliance with regulatory requirements, and security specialists can identify weaknesses in the company's IT infrastructure.

We recommend that you focus on the assessment of digital threats and their impact on business: dependence on IT has become even greater, and with it the value of information and data assets. As an example, here are a few threats to consider.

Social engineering

Social engineering attacks often lead to incidents. Such an attack can result in an adversary penetrating the corporate network and undermining the resilience of the infrastructure. In 2019, a German energy company lost €220,000[2] after the adversaries obtained the CEO's details, recreated his voice and convinced a high-level employee to transfer the money out of the company's account.

Note that email, phone and messenger tools are still quite popular with cybercriminals. Don't underestimate this type of threat: according to Sber, there was a 45% increase in email attacks and a 67% increase in SMS attacks in 2020.

2. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case // The Wall Street Journal.

Data leaks

Data leaks are as damaging to finances as they are to a company's reputation. The causes of leaks may be varied: unethical employee behaviour, malware infection, negligent hosting of customer databases, etc. Furthermore, the switch to working from home has created new sources of threats. Just imagine, your little child or even a cat goes over to your unattended laptop and accidentally sends a sensitive email to a wrong recipient.

According to IBM Security, the average cost per leak incurred by companies is $4.24 million[3].

Assessing the threat of a leak is useful when auditing digital assets and finding vulnerabilities in them.

Fraud

Attacks on customers take a big hit on reputation. They can greatly and irreversibly undermine brand loyalty.

We have come across a situation where customer outflow increased ten times because cybercriminals managed to steal money through the organisation's website. This is a clear example of an indirect loss.

For companies providing services online, this threat should be classified as critical.

3. Cost of a data breach report 2021 // IBM Security.

Planning the measures

The aim of planning is to develop technical and organisational tools to ensure business continuity.

For this part, you will need to complete the following:

- revise preventive measures to reduce the risks of adverse scenarios
- change the approach to incident response
- establish an incident response team
- budget for BCM implementation: purchase of technical tools, policy changes.

The plans listed below are designed to prevent incidents and minimise their impact, we recommend these as a priority:

- Business Continuity Plan **(BCP)**
- Incident Response Plan **(IRP)** and Disaster Recovery Plan **(DRP).**

When developing a BCP, we identify key business continuity parameters, which may include:

Recovery Time Objective (RTO). The time given to restore business functionality or service availability in the event of an incident.

Recovery Point Objective (RPO). The amount of acceptable data loss.

Service Delivery Objective (SDO). The level of service to be provided before full recovery. For example, in case of an incident, the business will have to operate at a reduced capacity.

BCP helps you find a balance by achieving optimum values for each of these parameters. This makes business continuity a measurable and manageable objective that is accessible to most departments and divisions, from logistics and accounting to IT and cybersecurity.

The IRP and DRP outline target scenarios and courses of action that enable the company to minimise damage caused by an incident and reduce the time taken to deal with the consequences.

The two plans address the following business needs for incident handling:

- clarity and management of documented procedures
- coordination and management of communications
- staff awareness and readiness to act swiftly on the given process.

Our practice shows that people are naturally less receptive to long bureaucratic documents and tend to base their work on verbal agreements and habits developed over the years. As a result, plans, guidelines, and policies end up being stacked on the shelf, gathering dust until the auditors drop by. In our opinion, this approach should be long abandoned in favour of developing policies that reflect real patterns of behaviour. These templates should also be implemented in automated systems as processes that create a natural 'gateway' for the algorithm and a set of employee actions. All documentation should be compiled into an accessible guide that everyone in the organisation can understand – refer to the steps in Sections 1 and 2 of this guide.

Note that your incident response team is more effective at deploying the new measures. If you lack such a team, we advise you to establish one before proceeding. Start by:

- identifying key stakeholders (PR, legal, HR, IT, management, customer support) who need to be informed and involved in the event of an incident
- compiling a stakeholder contact database and keeping it up to date.

Given the increasing dependence of business on technology, it might seem that the most obvious thing is to buy the right hardware and software. But in many cases, it is more cost-effective to develop emergency procedures for manual tasks than to deploy costly solutions to keep processes running for hours or even days at a time.

Oftentimes, the damage from an incident can be reduced not by technical measures, but by organising an adequate and timely response

By contrasting the potential damage from an incident with possible scenarios of events, a company can choose the optimal measures to keep processes running smoothly.

The following is a real case example of a chaotic reaction, which in turn exacerbated the threat, and made its consequences far more dangerous.

A few years ago, an online taxi service suffered a leak because employees submitted their login credentials on GitHub. Attackers found the source code and were able to get into the repository, where they found the data of 57 million customers. As a result, the company had to pay a ransom of $100,000 to prevent the disclosure of data. However, the story still went viral and damaged the reputation of the service. In addition to the ransom, the company had to pay a fine of €400,000[4].

4. Uber concealed huge data breach // BBC.

Deployment and testing

The purpose of implementation and testing is to create a BCM system that involves almost all departments, so that PR, legal and other specialists can get involved at different stages in responding to a cybersecurity incident.

By this stage, you need to:

- approve the final budget for the purchase of the necessary tools
- decide on service providers
- launch the incident response team
- arrange staff awareness events dedicated to business continuity management
- see how the measures work in practice, assess their weaknesses and make adjustments.

Do not rush to implement all the measures, this is a gradual process that needs the attention of the incident response team.

Always use incident modelling to test the measures you want to implement. For example, after migrating your data to the cloud, you can suspend the main (production) site for a while to see how well the cloud service provider handles the workload. Perhaps, this will give you an early warning sign that you need to switch service providers in order to avoid future interruptions in the event of an incident.

Don't forget to regularly test your incident response team. It makes sense to send them off to cyber trainings and encourage the sharing of experience with experts from other companies. An example of such an event is the annual Cyber Polygon training, where organisations test their level of cyber resilience and share best practices with the global community.

If you want to assess your resilience to phishing, it's a good idea to bring in external experts to conduct training attacks. There are services available out there to help you simulate a real threat, find weaknesses in existing defences and correct them.

The test results will help you identify the most vulnerable groups of service providers, company assets, and employees. Use this insight to follow up with targeted measures.

Another effective way of looking at your cybersecurity measures is through the eyes of an intruder. This includes special Red Team exercises: external experts simulate a real attack on the company's infrastructure and use all possible vectors to compromise it. The objective of the intruder could be anything from gaining access to sensitive data to carrying out transactions on behalf of the user. These exercises will allow you to find security gaps before they are exploited by cybercriminals.

Conclusion

The implementation of BCM is a multi-stage process with almost every company department doing their part. Each step has to be thoroughly elaborated and nothing must be left out. You need to do a detailed inventory, classify your assets, investigate internal and external risks.

The measures should be developed so that they can be applied even in the most unforeseen situations. In the next section, we will explain how to build an effective incident response system using real cases from our practice.

Incident response: the key to business continuity

Key ideas

Incident handling is a cyclical and continuous process. It may modify each time there are changes in the company's infrastructure.

When an incident occurs, the following actions are taken to deal with it:

- incident detection and analysis
- containment and recovery activities
- actions in response to the incident, including a review of current tools and processes.

By detecting early signs of an incident and taking immediate action, it is possible to minimise and even eliminate its impact. At this stage, it is important to gather as much information about the incident as possible: when it happened, what exactly happened and which systems are affected. The collection of artifacts and evidence is the foundation for further work.

This process usually takes place alongside with an investigation, i.e., a more in-depth analysis of all the circumstances that can help explain what happened.

Once the incident has been identified, the next step should be to contain it: analyse the countermeasures, assess the real extent of the consequences and eliminate the cause. Then, it is important to understand when the processes affected by the incident can be resumed and business operations returned to normal.

The final stage is learning from your mistakes. This requires a comprehensive look at the response actions to see if all the employees were prepared for the incident and if their knowledge and expertise were sufficient to effectively deal with the threat in the moment as well as maintaining a seamless operation of the infrastructure.

Unfortunately, there is no single approach for each and every incident. The threat landscape is constantly changing; thus, your measures and tools have to keep up with these changes, and your staff will require regular cyber literacy training.

To illustrate the multitude of incidents in the digital environment, our experts have compiled a series of real case studies. Each one comes with guidance to help you develop a clearer understanding of how to act in any given situation.

In the previous section we looked at the preliminary stages of implementing BCM, from examining the factors affecting the business to creating crisis response plans. Now, let's talk about what to do if an incident has already occurred.

Incident detection and analysis

The first step of incident response is always to detect signs of an incident.

Here is what needs to be done in this case:

01. Gather the details of the incident:

When did it occur?

What exactly happened?

Who discovered the incident and how?

Which systems were affected and what measures have already been taken?

Use this step to collect as much evidence and artifacts as possible, they will be helpful in analysing the incident.

02. Report the incident to the response team.

The course of actions in this case depends on how your company's processes are set up and the severity of the incident.

When business continuity is under threat, the incident should be reported to the response team, which is comprised of key stakeholders (legal, PR, cybersecurity, IT, customer support). In Section 2, we cover the process of setting up such a team. If you do not already have a response team, you can outsource this function to specialists.

For non-critical incidents, alerting a security and an IT specialist should be enough.

03. Compile and organise the information gathered about the incident.

It is a good idea if your company already has an incident report template. But even if there is no such document, try to record all the data in writing so that it can be passed on to digital forensic specialists or used as evidence in court.

04. Estimate the extent of the compromise.

At this point you need to find out how many workstations have been affected, what consequences the incident might have caused, what business processes are disrupted, and how much time and money it will take to neutralise it. It is equally important to think about the reputational damage and find out if customers or contractors have been affected, or if the incident has been reported in the media.

Sometimes, the best action is inaction. Not every incident will result in a financial loss serious enough to require a response procedure. Examples of such incidents are isolated incidents where an employee fails to log in to the system. These cases need to be recorded and monitored, but there is no need to go through all the stages of the response process.

Remember that some countries have regulations and requirements for security breaches. Particular attention is focused on incidents involving personal data. For example, in the event of a leak, regulators in some countries oblige the company to inform all affected parties: if an intruder has accessed an individual's personal data, the owner of the system where it has been stored must notify that individual. Occasionally, the owner of the system must also report the breach to state authorities.

Containment of the incident and recovery of operations

At this stage, it is important to understand what to do to minimise the impact of the incident. Here's where to start:

01. Assess your current measures.

Ask yourself the following questions:

What is the real scale of the incident as of now?

What has already been done to reduce the impact of the incident on the business processes?

02. Try to isolate the systems that may be infected.

If individual components and systems cannot be isolated, intensify monitoring so that the threat is not overlooked.

You will have to operate in total uncertainty, because at this stage you may not have a complete picture of the incident, yet the dangerous consequences still need to be contained.

Also note that the investigation procedures can be initiated at this stage. However, in some situations, it is acceptable to leave security gaps in place during the investigation, with increased monitoring of the unprotected systems. This will help to better understand the causes of the incident and even uncover other cybersecurity issues. The problem may be much more serious than is first thought.

An example of such an incident could be a hacker attack: leaving a backdoor for an attacker to exploit can allow you to monitor their behaviour and detect other infected components.

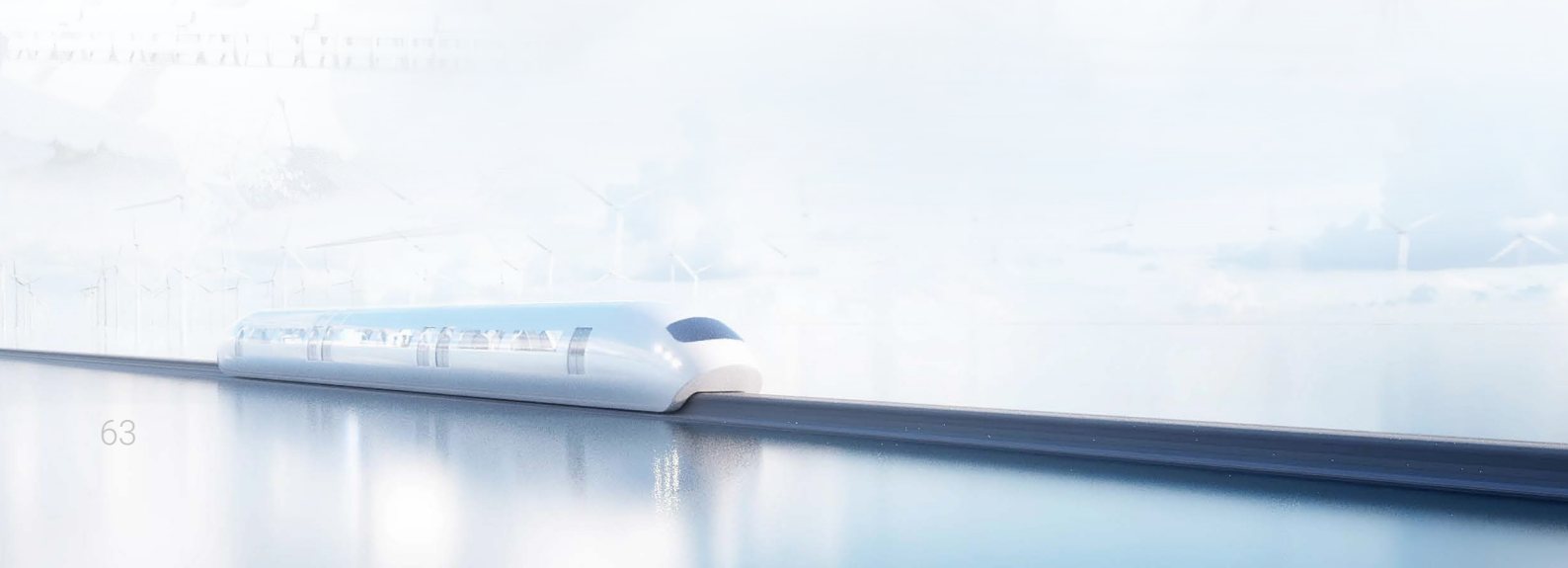
However, it is best to avoid doing this on your own and to contact a computer forensics expert who will ensure that the threat does not spread across the network.

03. Check all systems and see if the incident has spread to the entire infrastructure.

It is important not to get fixated on one thing and look more broadly at what has happened. This will protect you from an unexpected incident in another component. For example, an attack on an accountant's computer could spread to the entire corporate network. But the spread of the attack can be missed if you focus on protecting just that one device.

04. Eliminate the cause of the incident.

Close the security breach and make sure that the attack on the company's systems is contained.



05. Find out if the systems affected by the incident can be recovered.

There are situations when individual system components are permanently damaged – the company should be prepared for this. You need to plot your way forward, given that some infrastructure components or critical data have been lost.

As a result, you should have the foundation for a safe recovery of business processes.

Recovery is primarily aimed at getting systems back up and running if they have failed, or simply to get back to business as usual.

Make sure you also do the following:

1. Find out when the business processes affected by the incident can be resumed. It is worth considering how long it will take to investigate and clarify all the essential details that will serve as evidence. Sometimes it is necessary to allow specialists more time to get a better understanding of the system in which the failure occurred. In this case, the system may remain isolated for a while.
2. Restore compromised systems to their original state using backups.
3. Check that all affected systems have received the necessary updates and patches.

Once the processes are in place, you can move on to reviewing existing measures and analysing the incident response procedure in more detail.

Reviewing current processes and tools

Our project experience shows that companies often neglect to work on errors and stop the incident response as soon as operations are restored. We advise you to analyse what happened and review the incident management approach as a whole.

Here is what you can do:

01. Take a comprehensive look at the incident to identify areas for improvement.

Think about what changes to organisational measures would be worthwhile, which equipment needs to be purchased and which needs to be abandoned. Answer a few general questions to help you make a clearer plan of action:

Were all your staff prepared for the incident?

What mistakes slowed down the incident response process?

Did you and your staff understand the course of action? Did they follow it?

Do your employees have enough knowledge to effectively respond to cybersecurity incidents?

02. Survey the team that was involved in the response process.

Refer to the questions above. This will help you to comprehensively assess what happened and get a clearer vision on the gaps in the response process.

03. Review your continuity management and incident response documentation.

These are the questions to keep in mind:

- Are there any errors in the description of the algorithms?
- Is the text of the documents clear to all staff, without complicated clauses written in bureaucratic language?
- Does the documentation cover the issues that have arisen in the course of addressing the incident?

If such documentation does not exist, it is worth developing one that takes into account the difficulties encountered in responding to the incident.

04. Repeat the audit of your digital assets.

Make sure that none of them are outside the scope of control.

It is also advisable to track changes to external and internal infrastructure that have occurred during the incident.

05. Determine what measures and tools can be used to reduce the likelihood of such incidents recurring.

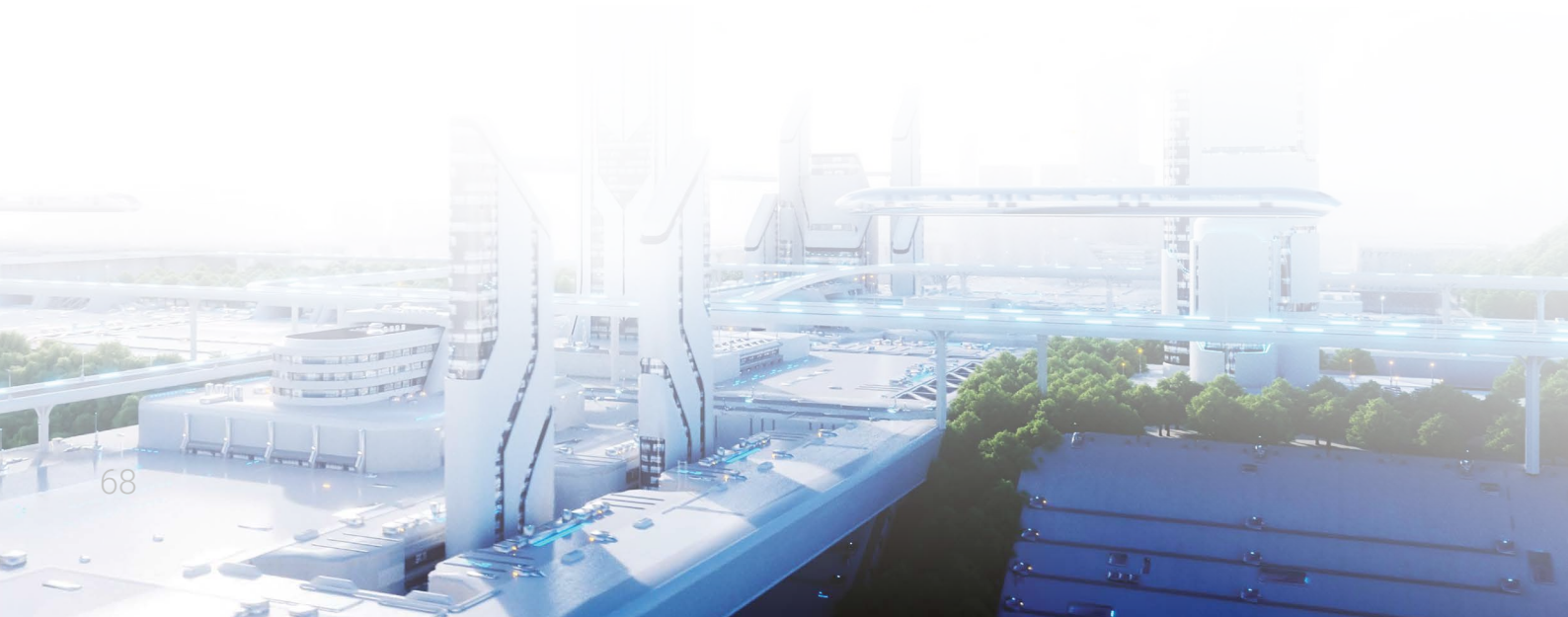
You need to work on the mistakes and answer the questions:

What weaknesses are found in existing security measures (security policies, tools)?

How can the business be protected from similar incidents in the future?

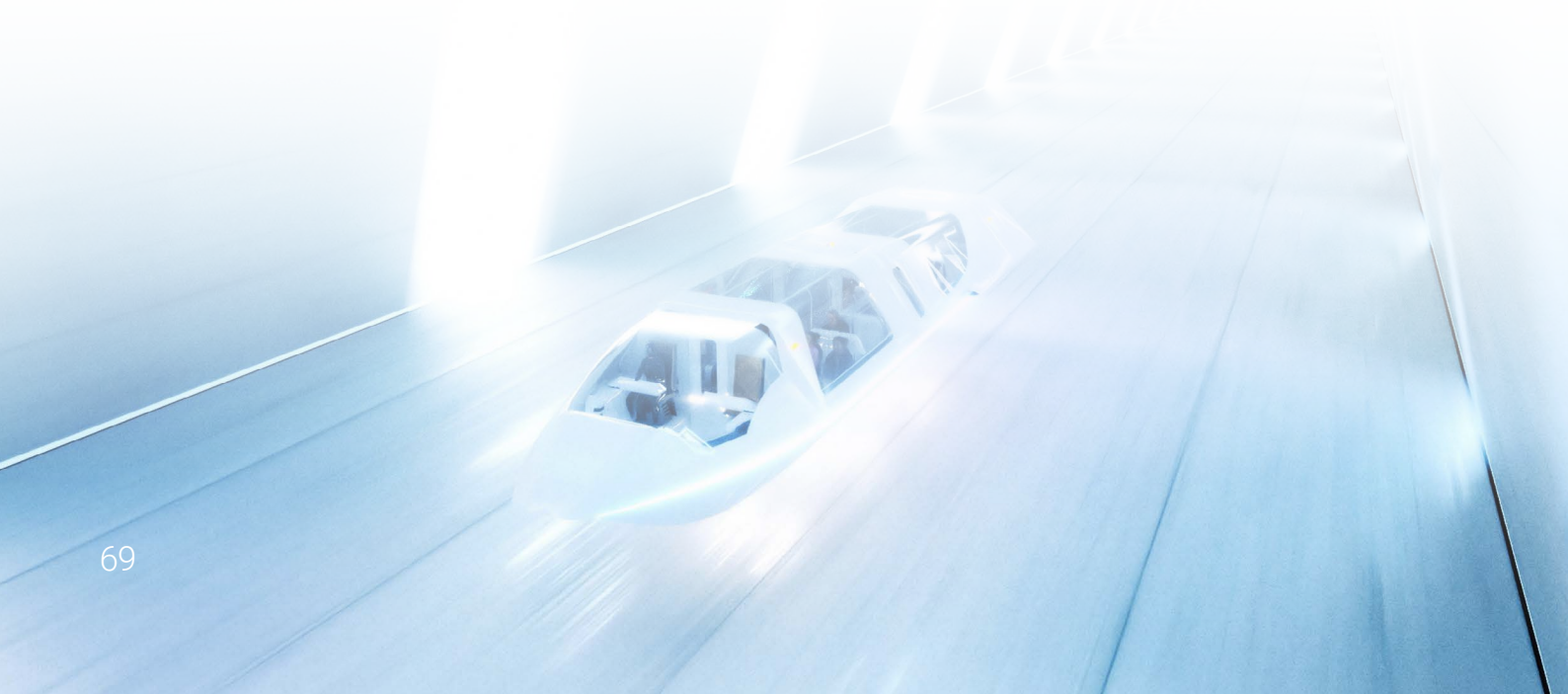
06. Figure out what you need to change in regard to educating your employees.

In this step, you can introduce relevant training programmes: practical exercises, cyber literacy webinars, etc. For technical experts, participation in cyber exercises can be useful as a way to test their skills, improve their qualifications and share experiences with colleagues. Such exercises can be organised by specialised cybersecurity companies. Alternatively, there are online events where participation is free of charge.



The discussions following the work on the incident can be summarised in the following table.

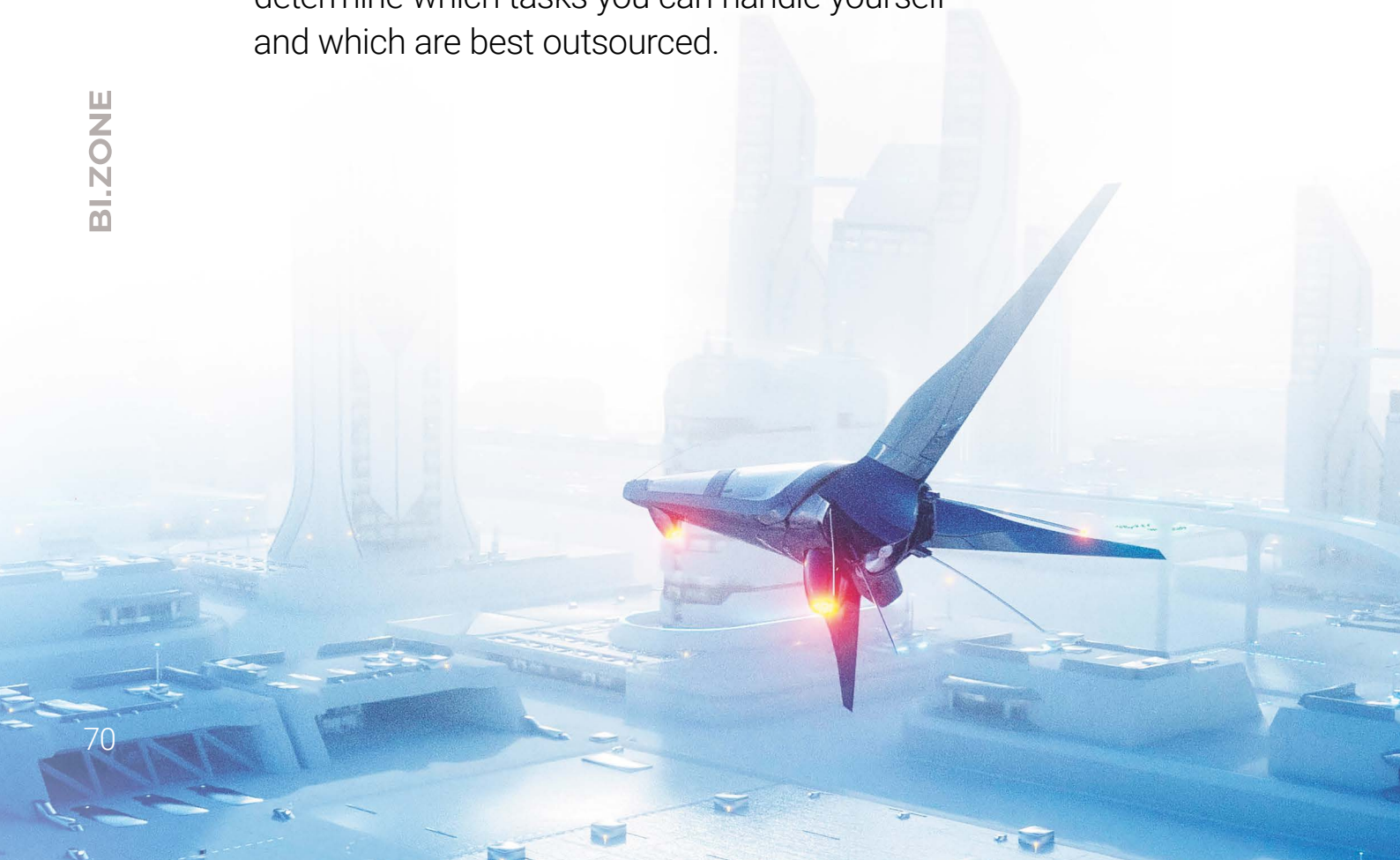
What can be done/ improved	Responsible person	Due date	Comments / references to the task
Develop, deploy and implement a password policy for your web applications	Full name, position	dd.mm.yyyy	
Identify critical systems and processes, analyse relevant threats	Full name, position	dd.mm.yyyy	
Conduct a security assessment of the critical systems	Full name, position	dd.mm.yyyy	Consult external experts
Consider establishing a Security Operations Centre as an internal division of the company or as a service provided by a vendor	Full name, position	dd.mm.yyyy	



Staying on guard. How to prepare for different cyber incidents

As stated above, there is no single incident response approach. However, it is possible to prepare for some events in advance and thereby minimise potential damage. To help you do this, we have compiled a set of recommendations from BI.ZONE experts, backed up by examples of cybersecurity incidents and statistics from our practice.

Do not attempt to cover all types of events in one afternoon – it would be more effective to study each scenario separately and immediately check how things are going in your company. This way, you can identify gaps, plan your next steps and determine which tasks you can handle yourself and which are best outsourced.



System intrusion

We often encounter situations where a company focuses on technical protection of the perimeter but does not care at all about monitoring. However, it is impossible to ensure absolute protection – there are still gaps in the infrastructure that can be exploited by attackers. As a result, the company is unprepared for an attack that can breach the perimeter defences.

To increase the likelihood for the business to handle an incident, we recommend taking a comprehensive approach to security: allocate a budget for software, but also remember to implement organisational measures and build a response team. Evaluate your resources to see if you can conduct regular security audits of your IT perimeter internally.

If you suspect that your corporate network has been compromised, contact digital forensics experts. Do not ignore their advice, or you may expose your infrastructure to a second attack.

Ask yourself

- Does your company have a department that deals with cybersecurity issues?
- How does your cybersecurity team develop skills and learn about current threats?
- Is there a balance between technical and human resources?

Example

Employees at Company A detected suspicious activity on their network. It was soon discovered that the attackers had gained access to a privileged account on the computer which administers the company's entire network. The attackers could have potentially disrupted all of the organisation's business processes and stolen funds from its accounts.

The investigation revealed that a well-known cybercriminal group called Silence was behind the attack. The intruders were able to penetrate the critical system because an employee working on it opened a Word document containing malicious content. From the compromised machine, the attackers infected the organisation's entire network with several remote access tools.

Countermeasures and consequences

Our experts managed to block access to the organisation's network and removed the malware from it. The company also received detailed advice on the need to build cybersecurity processes, assemble a full team of cybersecurity specialists and set up regular security audits.

A few months later, the company reported a repeat attack on its systems and the theft of €43,000. An investigation revealed that the attackers were the same Silence group and that the attack was due to unresolved security flaws discovered earlier. None of the recommendations were implemented.

Mistakes

Company A focused on building its perimeter defences and invested in expensive security equipment.
At the same time, it did nothing to organise monitoring and to hire qualified specialists who could maintain the security systems.

As a result, the company made some serious mistakes in the preparation phase.

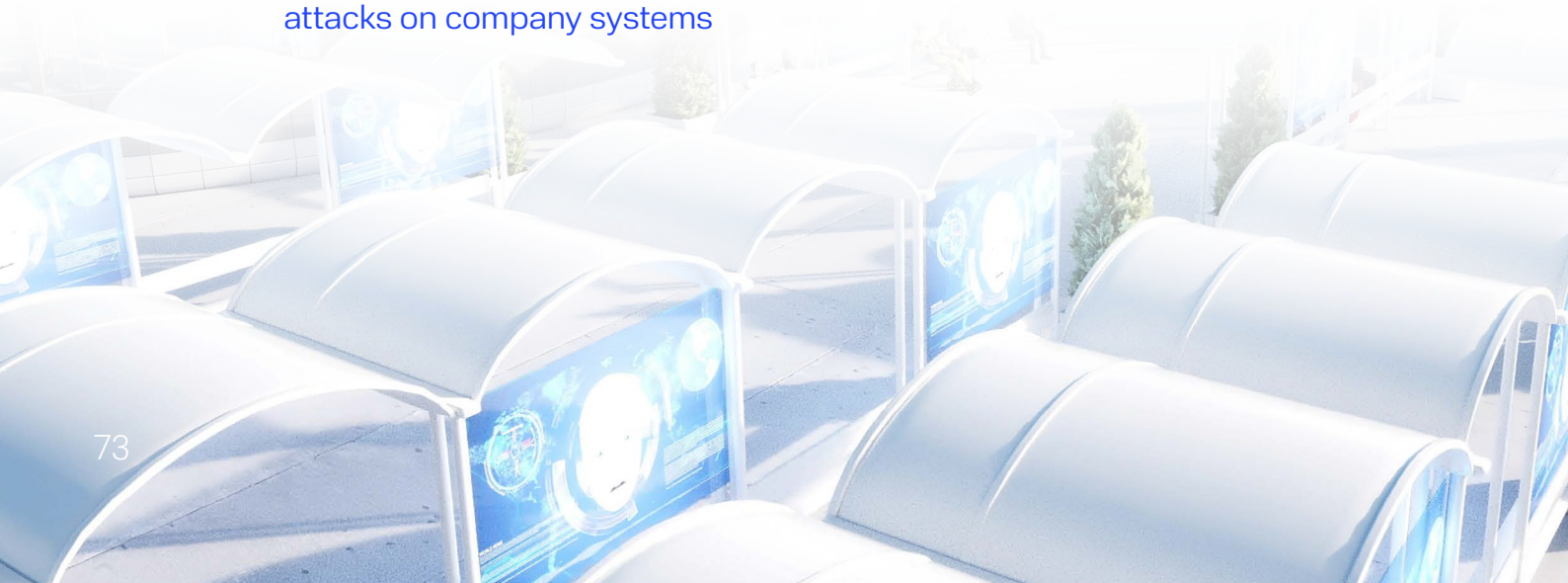
Even more significant was the company's failure to follow expert advice and take measures to protect against a cyberattack, so the incident repeated itself.

in 31%

of our external pentest projects, we successfully gained access to the internal network

€43,000

incurred in losses due to repeated attacks on company systems



Fraud against company clients

It is difficult to predict an attack which uses your brand.

However, with a well-designed incident response process, you can plan for such an event effectively and avoid customer outflow, reputational damage and financial loss.

Here's what you can do to safeguard your customers and protect your brand's reputation:

- Analyse the risks in the digital environment that pertain to your brand's reputation and interactions with customers. Factor them into your crisis planning
- Look into possible attack scenarios against your customers. You can do this by researching news articles about the attacks on the customers of other companies in your industry
- Search for fraudulent websites and other sources disguised as your brand. This is difficult and too time-consuming to do on your own, but you can always outsource brand protection to external experts.

If an incident has already occurred, try to get the IT, cybersecurity, product marketing, PR and customer support involved as early as possible. This way, you can build a chain of communication with the public and minimise risks to your reputation.

Do everything you can to stop the malicious actors. Warn your users about the threat. Report honestly. Tell people that your brand is being used by criminals and prepare a detailed guidance on how to avoid the fraud.

Ask yourself

? Have you thought about how cybercriminals might target your customers in your name?

? Does your company have a clear plan of action in case cybercriminals attack users and undermine public trust in your business?

Example

Last year we worked with Company B which was affected by cyber fraud.

Company B owns a large classifieds platform. The attackers created fake advertisements for the goods being sold on the platform and directed potential customers to phishing payment pages.

The victims of the scam concluded that the platform itself was involved in the scam and threatened to sue its owners.

Countermeasures and consequences

To stop the attacks, Company B made the decision to ban the exchange of non-official links on its website. But the fraudsters found a way to bypass the restrictions: they continued the dialogue with their victims on social networks and messengers.

As a result, the company's reputation suffered a great deal: users lost trust in the marketplace and customer outflow increased tenfold over the period. In addition, the company incurred losses in the form of several legal settlements.

Mistakes

Company B did not monitor phishing sources created by the criminals. The company probably hadn't even considered such a threat when laying out its security strategy.

There was also insufficient attention focused on protecting users during the response phase, so the scammers quickly found a loophole to continue their attacks successfully.

By avoiding such mistakes, the company could have retained more of its customers.

60%

of companies audited by our team
have a low level of internal infrastructure security

Information attack on the brand

An attack is just as likely to come from the media in the form of negative PR or suspicious publications from questionable sources. These areas must also be adequately monitored for any early signs of a full-scale misinformation campaign and its spread. These tasks can be outsourced to external brand protection specialists who are able to provide a better coverage of the media sphere.

To avoid getting caught off guard, you need to have preliminary strategies in place to respond to the most probable information attacks. Here are some actions to help you do so:

- Make a prediction of possible information attacks that could be launched against your company by dishonest competitors or rogue adversaries
- Develop some response options for different types of attacks, outlining the course of action that will deflect them. It is important to consider how to communicate the information that will clear up or prevent the spread of misinformation. It is advisable to have a number of response options to select from
- Prepare message templates for all corporate media channels such as blogs, social media and mass media in the event of an information attack.

If you have detected an information attack, first formulate a response and publish it on the company's official website.

Make sure the refutation is accessible and widespread: the information that benefits the brand should be on the surface, and the mitigating content should quantitatively outweigh the negativity.

Ask yourself

- Does someone in your company monitor your brand presence online and in the media?
- Does your PR department have a response plan in case of an attack on the brand?

Example

Some adversary posted a fake press release in the media on behalf of Company C announcing the resignation of its CFO. By the time the company became aware of this misinformation, it was too late to initiate an adequate response and counter the damage.

Countermeasures and consequences

The inaction of the company C caused its shares to plummet by almost a quarter. The financial loss due to the incident is estimated at several billion dollars.

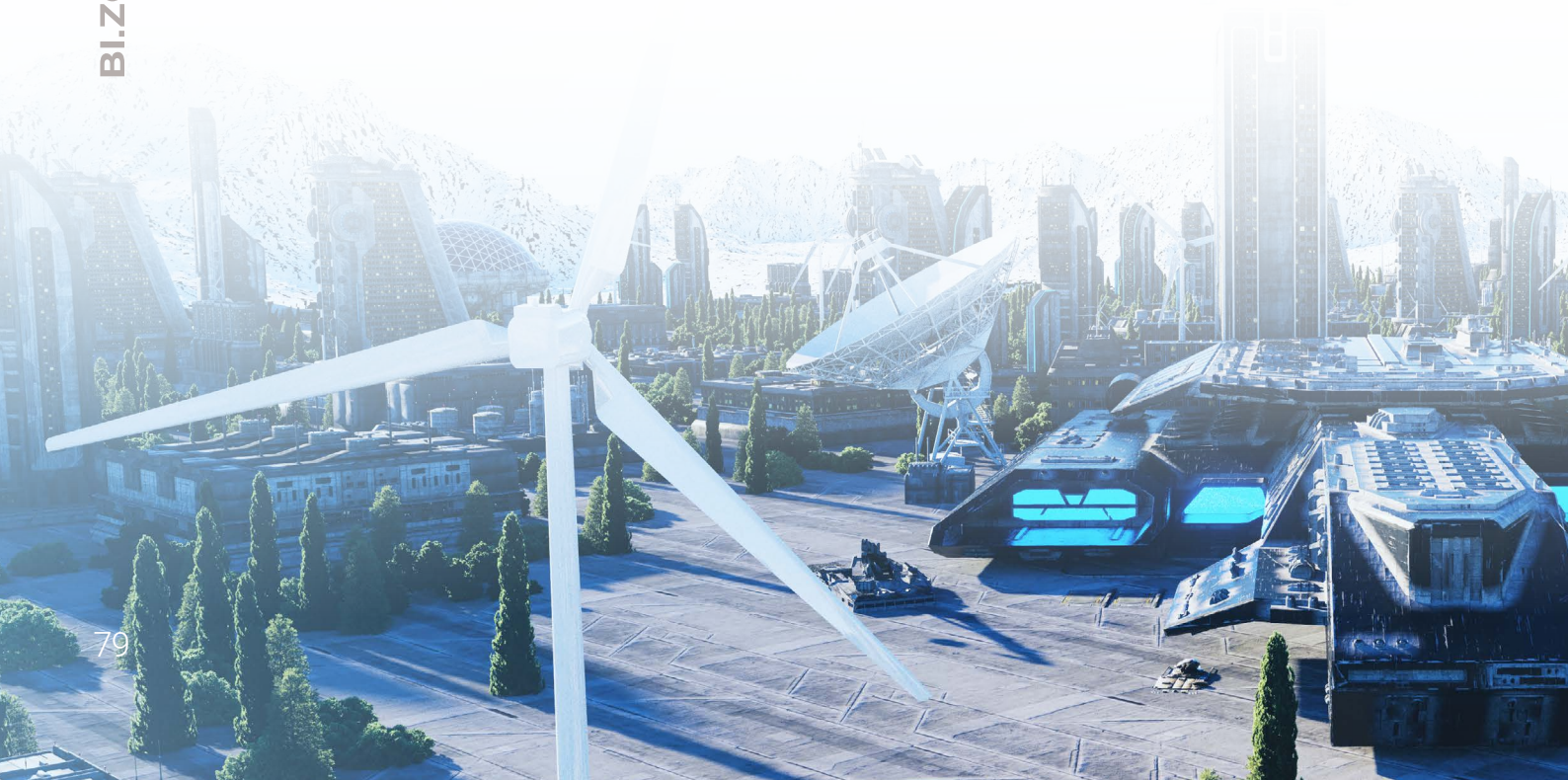
Mistakes

Company C did not react to the incident in time and suffered losses as a result.

The main problem with information attacks is that they are extremely difficult to predict, as you may not have enough resources or monitoring tools to do so.

The mistake is that the business continuity management system does not take into account risks such as negative PR.

Because of the information attack, Company C's shares dropped by nearly 25%



Issues concerning the security of a company's web application

The best way to respond to a web application security incident depends on the type of used malware and its sophistication. However, there are some general recommendations that can help optimise the response process.

- Continuously monitor changes on your external IT perimeter
- Conduct regular targeted penetration testing of resources when new applications are released, sites are changed, or service versions are updated
- Conduct regular inventory of digital assets
- Check open sources for forgotten assets: servers with outdated and vulnerable software, domains, admin panels with default passwords, etc.

If an incident does occur, focus on minimising the consequences. Install security updates, isolate the infected system component.

Ask yourself

? Do you carry out a review of the company's external infrastructure security? If so, how often do you do it?

? Does your company have a well-established process for finding vulnerabilities on the external perimeter?

? Would you be able to detect a vulnerability that has existed on the perimeter for a short period of time (2-7 days)?

Example

When doing external penetration testing for Company D, we discovered a suspicious page and a script on one of its websites. Upon closer inspection, it turned out to be a web shell*.

Attackers typically use web shells to control compromised sites and web servers, which includes executing console commands, accessing the file system, and so on.

The presence of a web shell means that the web application has already been compromised. The investigation revealed that the site had been compromised as a result of a massive cyber attack.

Countermeasures and consequences

Penetration testing experts relayed the information to Company D.

The analysis revealed that attackers had identified a vulnerability in the web application using publicly available information sources (Shodan, Censys).

The consequence of the attack was that the web application's resources were hijacked to mine cryptocurrency. The attackers also had the opportunity to cause direct financial damage, steal sensitive data, or encrypt data on the server to demand a ransom for its decryption.

* Web shell is a malicious script, a backdoor that allows attackers to control other people's services, steal passwords and perform other illegitimate manipulations.

Mistakes

It took a long time for Company D to realise that an incident had occurred in its infrastructure – this created additional risks of the threat being spread across the network.

This is often due to insufficient monitoring of the assets located on the external IT perimeter and a lack of processes to identify vulnerabilities on a regular basis.

in 70%

of our internal pentest projects, we successfully obtained domain administrator rights

Surveillance by means of covert information gathering devices

Hardware attacks are still relevant, so we should not discount their severity. The following steps should help you avoid becoming a victim of such an incident:

1. Develop a procedure for reporting suspicious activity in or around the office
2. Arrange routine checks for hidden cameras, voice recorders etc.
3. Provide a short training session for staff about the threat of spying devices. Explain that the presence of unauthorised persons on company premises could pose a threat to security
4. Post warnings around the office about the need to alert security or IT if an employee notices anything unusual about their equipment: mobile service disruptions, Wi-Fi glitches, or the presence of unusual devices
5. Make sure security cameras in and around the office are working correctly.

If you happen to find a spying device in your office, contact your security team to carefully remove and examine it. Check CCTV cameras and access logs to identify the intruder who was at the premises and installed that device.

Ask yourself

- Do you have video surveillance installed on your company premises?
- Do you factor hardware attacks into your company risk profile?
- Do you monitor who visits your office and when? How easy is it for an unauthorised person to enter your company premises?

Example

During a routine inspection of Company E and its premises, a mobile phone interception device known as IMSI-catcher was found planted near the office.

Employees had previously complained about a poor mobile signal, which only confirmed that the device was tampering with the phone reception.

Countermeasures and consequences

As soon as the device was discovered, it was reported to the head of security. The device was dismantled. In this case, no processes were affected, but the attackers may have had information about some internal decisions and sensitive phone conversations.

Mistakes

Company E responded quickly to the incident. However, it is worth noting that not every organisation checks for such devices in and around the office. In addition, video surveillance has its blind spots, so it is difficult to track down an intruder.

A surveillance device may remain undetected for quite some time. The device might be used by dishonest competitors or criminals to gather sensitive data to attack the victim, so it's a big mistake not to factor in the risk of such an attack as part of your strategy.

Loss of access to data due to security problems

Incorrect configurations, a lack of password protection or the use of default passwords are among the most common vulnerabilities associated with databases. It is important to be aware of the typical gaps and take them into account when analysing the security of your systems.

Here are some tips to help protect your company's databases from hackers:

- Audit your external perimeter. Ideally, this process should be continuous
- Check that there are no resources on the external perimeter with insecure configurations, such as default passwords
- Back up important databases
- Do not store user passwords in plain text
- Conduct targeted penetration tests when launching new services or changing websites. Organise thorough monitoring of the DBMS.

If an incident does occur, reconsider how the databases are stored and accessed. Repeat the audit of your digital assets and compile a risk profile for them.

Ask yourself

? Do you keep records of digital assets: customer databases, electronic documents? Can you say with confidence that none of them are out of your scope of control?

? How often do you conduct an audit of your digital assets?

Example

When doing external penetration testing for Company F, a MongoDB database was discovered on one of its websites. All data in the database was encrypted except for one line: "All data is encrypted. To restore it, transfer Y btc to bitcoin wallet E. It will be deleted in N days". It turned out that the attackers had encrypted all the data in the database and demanded a ransom from Company F.

Countermeasures and consequences

The experts carried out an analysis which revealed that the database had originally not been password-protected, so anyone could gain read and write permissions to it.

Fortunately, the information contained in the database was not critical, so there was no damage to the client or their services.

Mistakes

Company F has overlooked the database. This happens when an organisation does not pay enough attention to IT perimeter control and digital asset inventory.

In addition, Company F did not even consider that such problems are common in MongoDB's default configuration.

Very often, attackers encrypt the really critical data, i.e., personal and user credentials, as well as system information – without which the service cannot continue to function.

Not all incidents involve threat actors – there are times when an unforeseen situation arises due to the fault or negligence of the contractors and employees.

Confidential data leaks caused by third parties

Security of communication channels with third parties is one of the most important areas of infrastructure resilience. Organisations often lose their vigilance and fall victim to the actions of insiders, partners or contractors.

Organise continuous monitoring of online resources to ensure timely detection of:

- employee accounts
- databases containing customer data
- snippets of source code
- access to the company's network
- sensitive information.

If you find that someone is selling sensitive company information, you can contact the offenders. By doing so, you can make sure that the data being sold is relevant and poses a security threat.

Ask yourself

- Are you familiar with the cybersecurity policies of the contracting companies you work with?
- Does your company have procedures for giving access to confidential data to third parties?
- Which data in your company requires special protection against insider leaks?

Example

A financial Company G was hit by a contracting agency whose employee tried to sell the victim's client base on the dark web. The database included the names, addresses and phone numbers of clients. Luckily, our experts were able to quickly detect the threat.

Countermeasures and consequences

Security specialists quickly identified the perpetrator and stopped him. Company G lost $55,000. The damage was relatively small thanks to the quick response from the cybersecurity team. The consequences could have been far more serious, since data leaks not only hurt finances, but also the reputation of the brand: the public loses confidence in the company, especially when it comes to personal data.

Mistakes

Company G encountered a problem on the side of the contracting agency, which had failed to enforce stricter access controls over confidential client data.

Such incidents are hard to anticipate, but the consequences in such a situation can be mitigated if the contractor's responsibility is clearly outlined in advance.

Sensitive data leaks due to employee negligence

A leak in the transfer of sensitive data can occur not only through the fault of third parties, but also through your own employees who are unfamiliar with the rules for the secure transmission of information.

The following steps can help reduce the risk of confidential data being leaked due to employee negligence:

- Evaluate the existing technical data protection measures when transmitting data to third parties. Check that these measures help to ensure a sufficient level of security. You can bring in external experts to test them
- Prepare organisational measures if you don't already have them in place. Develop detailed policies for secure data transmission. It is important that they are not overloaded with easy to understand. You should also try to keep the process as simple as possible, because if it's too complicated, employees simply aren't going to follow the instructions anyway
- Brief your employees and help them understand the basics of cyber hygiene.

If an incident occurs, try to remove the data from the public domain as quickly as possible. Contact the owners of the resources where the sensitive data has been leaked to.

Such leaks are often publicised in the media. Minimise reputational damage by engaging PR specialists in the response process.

Incident analysis can be made more effective with the help of external digital forensics experts. They will have the expertise to gather information that will be useful in litigation, for example, if you need to prove that your employee was involved in the incident and to assess and recover damages.

Ask yourself

- Does your company have procedures in place for the secure exchange of confidential data?
- Does your company have training sessions teaching employees how to share data safely?

90%

of companies do not use encryption mechanisms on their employees' laptops

only 25%

of companies encrypt corporate information on flash drives

Example

A sales employee at Company H sent out a service file to a customer but not in the way prescribed by the company guidelines. The data ended up in the public domain as a result of this breach of conduct.

Countermeasures and consequences

As soon as H learned of the incident, it launched a response and investigation process which involved internal cybersecurity specialists and external digital forensics experts.

The breach was resolved. Although business processes were not affected in this case, the incident had a negative impact on the company's reputation in the eyes of the counterparty that first noticed the breach.

Mistakes

Company H was affected as a result of an employee failing to comply with the existing security requirements. Such incidents occur when individual users have insufficient cyber literacy. Sometimes employees are not even aware that the company has a specific procedure for secure data transmission.

An attack on the company's external infrastructure caused by human error

External infrastructure is often the weakest link in many companies: our research shows that external infrastructure has a low level of security across all industries. This is because the external infrastructure is difficult to monitor and not everyone has the resources to continuously scan for security breaches on the perimeter.

To minimise the risks of such incidents, it is advisable to take the following measures:

- Develop, implement and technically enforce a password protection policy, specifying the number and types of characters required in a password and its validity period
- Conduct cyber literacy training for employees. Introduce the basics of cyber hygiene and make checklists reminding employees of the rules for working with corporate resources
- Establish security controls for hardware and software configurations
- Make sure to back up your services to help restore them in the event of an incident.

If an incident has already occurred, the service will have to be reconfigured. It is important that more emphasis is placed on secure configuration. It is advisable to provide additional training to the employees who will be handling these tasks. After the incident, it is best to review the processes for rolling out the services to production.

Ask yourself

- Consider the passwords for your corporate accounts. Are there any weak passwords among them, such as default passwords ('admin', etc.), simple combinations of letters and numbers?
- Does your company have a password policy? Are all employees familiar with it?
- Is there a process controlling the setup of hardware and software in your company? Do employees always follow the setup instructions?

Example

Company I experienced problems due to a misconfiguration of an Internet-accessible service: an intruder was able to figure out the password for a service account and gain access to the company's server.

An investigation into the incident revealed that a service user with a simple password had been added to the operating system image the day before the service was rolled out. Moreover, the employee who made the change had not told anyone about it. The administrator who deployed the service did not follow the secure configuration guidelines which were to disable password access to the server and to set up other, stronger authentication methods using cryptographic keys.

Countermeasures and consequences

The incident was discovered by circumstantial evidence: the IP address assigned to the service was blacklisted by external reputation services, as reported by the company's digital reputation service provider. The service was shut down as soon as signs of malware were detected.

Internal cybersecurity and IT staff, as well as an external digital forensics expert, were involved in the response process.

The incident affected the business process: the company was unable to provide a service to customers based on the compromised service. This led to financial and reputational damages.

A service was deployed to restore operations using data from the backup. More attention was focused on configuring security settings in the process.

Mistakes

The cause of the incident at Company I was a breakdown in communication between staff members and a poor discipline on the part of the service administrator. The consequences could have been avoided by strictly following the requirements and instructions for a secure setup.

This incident also illustrates another common problem – the failure to comply with password policy requirements. Employees set passwords on their devices that are too weak, such as default passwords (e.g. 'admin'), making it easy for hackers to infiltrate the system.

Data leaks caused by an insider

Although insider threats are unpredictable, you can significantly minimise the risk of such a breach by doing the following:

- Design a system for keeping track of employees who have access to valuable company resources. A thorough logging setup can help
- Use a leak prevention system, i.e. data loss prevention (DLP)
- Sign non-disclosure agreements (NDAs) with employees. Prepare a security policy with approved procedures for handling confidential information.

If an incident has already occurred, try to focus on your company's public profile. To do this, involve the PR department and quickly think through a strategy for responding to the incident in the public sphere. This will reduce reputational damage.

Ask yourself

- Does your company have established procedures for granting access to relevant resources?
- Do you consider insider threats as part of your company's cybersecurity strategy?
- Can you verify at any time who has requested access to sensitive corporate information and when?

Example

In October 2019, advertisements for the sale of databases containing the personal data of allegedly tens of millions of customers of Company J were found on a number of themed forums.

The content of the databases indicated that the attack was carried out by an insider: the original data was stored in the Company J's internal resource, accessible only to a limited circle of its employees.

Countermeasures and consequences

After analysing the corporate computers of a group of company employees, it became clear that only the head of the sales sector in one of the company's departments could have been involved in the incident. Soon, under pressure from the evidence, the employee confessed that he had stolen the data to be sold on darknet forums. A total of several thousand customer data was leaked from that department.

The incident resulted in a significant overhaul of the company's cybersecurity processes and the delimitation of access to private information.

Mistakes

Company J has fallen victim to an insider. No one is immune to this, such incidents are difficult to predict. It is therefore important to carefully consider how best to handle such incidents.

Attacks via a third-party app

Using third-party software or outsourcing application development tasks is a normal practice. However, it is important to be aware of the security risks to keep yourself safe.

Quite a high risk is posed by undetected vulnerabilities and supply chain attacks, where attackers, for example, infect one company's software to attack multiple organisations that have installed it.

Here's what you can do to reduce the risks:

- If you are outsourcing the development of your software, make sure to carry out regular quality assurance. Repeat the procedure when updates are released
- Engage independent experts to audit the security of your developed software
- Do not forget that third-party software may contain vulnerabilities. Be sure to pull logs from applications and record anomalies in SIEM
- Check applications thoroughly and refer to the principles of SSDLC (Secure Software Development Lifecycle)
- Use the services of trusted developers and make sure to stipulate liability in the contract in case of such incidents.

If a threat is detected in relation to the use of a third-party program, carry out an investigation, either in-house or with the help of external experts.

Ask yourself

- Do you outsource the development of software? If so, do you regularly review the security of these programs?
- What measures do you take to ensure secure application development?

Example

Company K suspected that there was a problem with their system and asked BI.ZONE to analyse the security of an application created by a third-party contractor. The analysis revealed a backdoor through which the developer was slowing down the speed of the application, thereby forcing the company to sign up for additional technical support services.

Countermeasures and consequences

The contract with the third-party developer was terminated. But the client had already incurred a financial loss by purchasing additional support services.

Mistakes

Company K had not initially considered the risk of malicious activity from its contractor. A third-party software vendor has the ability to introduce backdoors, which makes the vendor not very reliable or trustworthy.

The biggest mistake was that Company K requested a pentest much too late – it should have been done at the time of accepting the finished software from the contractor, rather than some time afterwards.

Another problem was the lack of control over the development and implementation of the application.

18,000

public and private SolarWinds users affected by a supply chain attack[2]

2. US secret services created a group to investigate the cyberattack on the government. [Spetssluzhby SShA sozdali edinuyu gruppu...] // Forbes Russia

Conclusion

We advise you not to postpone building an effective business continuity management system. Try to assess your resilience to a variety of threats as soon as possible and start developing preventive measures.

We have prepared a quick checklist for you to take away.

- [ ] Recall when you last analysed the trends in the digital environment. If it was more than 6 months ago, it's time to update your analysis. This can help predict events that could impact your business in the short and long term.
- [ ] Keep an inventory of your digital assets, this will help you identify weaknesses in your IT infrastructure.
- [ ] Create a cyber incident response team. Identify key stakeholders (PR, legal, HR, IT, management, customer support) who need to be informed and involved in the event of an incident.
- [ ] Ensure that your company's data protection equipment is compatible with your business and performs effectively.
- [ ] Check the state of the technical defences: make sure they are all set up correctly and updated to the latest version.
- [ ] Ensure that the documentation that outlines the process for responding to cyber incidents is written in plain and simple language. Remember, the documentation should be relevant to your practices and processes, rather than just being for the sake of it.
- [ ] Adopt training exercises for your internal cybersecurity specialists.
- [ ] Develop a cyber awareness plan for line staff and supervisors.
- [ ] Consider outsourcing some of the digital transformation and cybersecurity tasks. External experts work with organisations of different sizes and industries all the time, so they would have a broader perspective on your challenges. Expert help can save you the most valuable resource – time.

Whether you want to build a cyber incident response system from scratch, audit your current processes and technical assets, or get some advice – our experts are here to help. Simply email us at info@bi.zone.

About us

BI.ZONE is an expert in strategic management of digital risks.

From start-up to corporation, we help organisations around the world to develop their business safely in the digital age. For small budgets we offer simple and automated solutions, for small teams we provide outsourcing, and for complex projects we prepare individual strategies based on 40+ of our own services and products.

We can assess your current level of risk, propose measures for improvement and optimisation, train your employees on working in the digital environment and provide round-the-clock support to your company.

Since its foundation in 2016, BI.ZONE has completed over 850 projects in finance, telecommunications, energy, aviation and many other industries. Our experts hold world-class certification, and we cooperate with a number of international organisations such as the World Economic Forum, INTERPOL, the International Committee of the Red Cross, SWIFT, CREST, the CyberPeace Institute.

Check out the range of solutions offered by BI.ZONE to help you build your cyber incident response system.

www.bi.zone

850+

completed projects

500+

successful investigations

40+

proprietary cybersecurity solutions

270+

protected clients

600+

dedicated professionals