Instituto de Auditores Internos de España

RiesgosClave

esfera consejeros

Cyber security, a systemic risk to watch over

When properly managed and supervised, risk becomes a competitive advantage

INDEX

About Esfera Consejeros ..... 2 Page

At a glance ..... 3 Page

Connectivity and cyber security ..... 7 Page

Assessing all the impacts ..... 14 Page

Governance framework ..... 21 Page

Cyber security as a competitive advantage ..... 27 Page

Internal Auditor's perspective: .... 31 Page

References ..... 34 Page

About Esfera Consejeros

Esfera Consejeros is an initiative directed at members of the **Audit Committee**.

This service provides analysis, synthesis and knowledge from a perspective of Internal Audit **rigor, quality** and **independence.**

Our objective is to provide the knowledge and transversal viewpoint characteristic of internal auditors, and thereby contribute towards enabling board members' oversight of the complex business world and its realm of risks

The service draws on different publications, **RiesgosClave, EnFoco and EnRuta**, which will be addressing relevant issues of business life at different levels and focus.

One aspect that sets it apart is **the Internal Auditor's perspective** with respect to the issue being analyzed: What are the key questions we need to raise? What concerns do the Internal Auditors have, and where and how do they act in order to provide assurance and comfort? All of these are questions that are relevant to the Audit Committee in its oversight and control duties

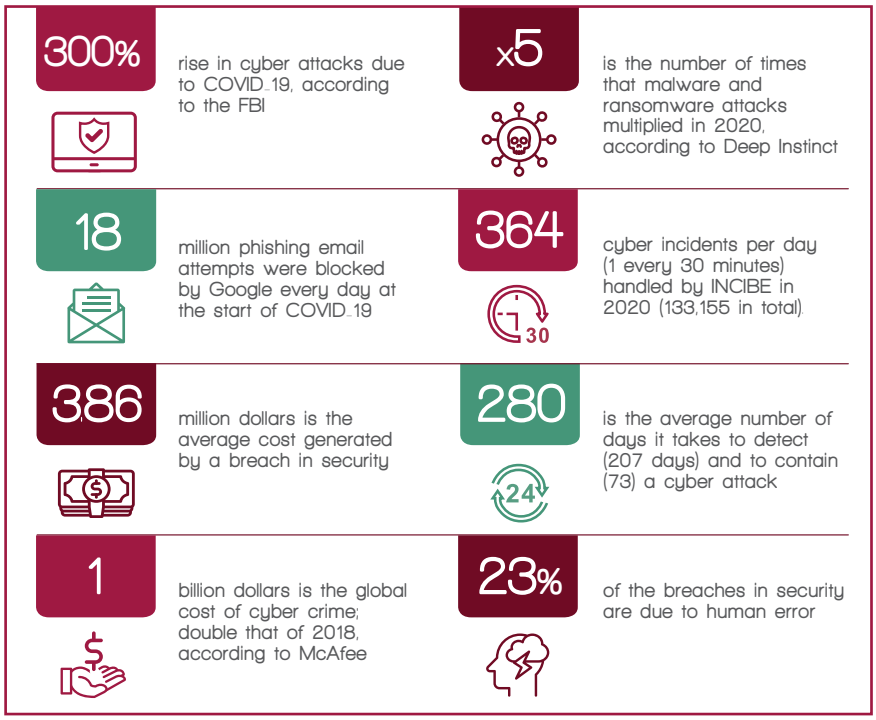
We trust that **Esfera Consejeros** will be useful to your organization.

May 2022

At a glance

Cyber security, a systemic risk to watch over This report provides a comprehensive overview to help Audit Committee members properly prioritize and monitor one of the greatest business risks. We outline key questions to understanding why the cyber security perimeter has expanded, its connection with other risks, the greatest threats, the costs of a cyberattack and what can help to mitigate it. The question is not whether there will be attacks, but when. We need to be prepared.

The risk of cyber security in data

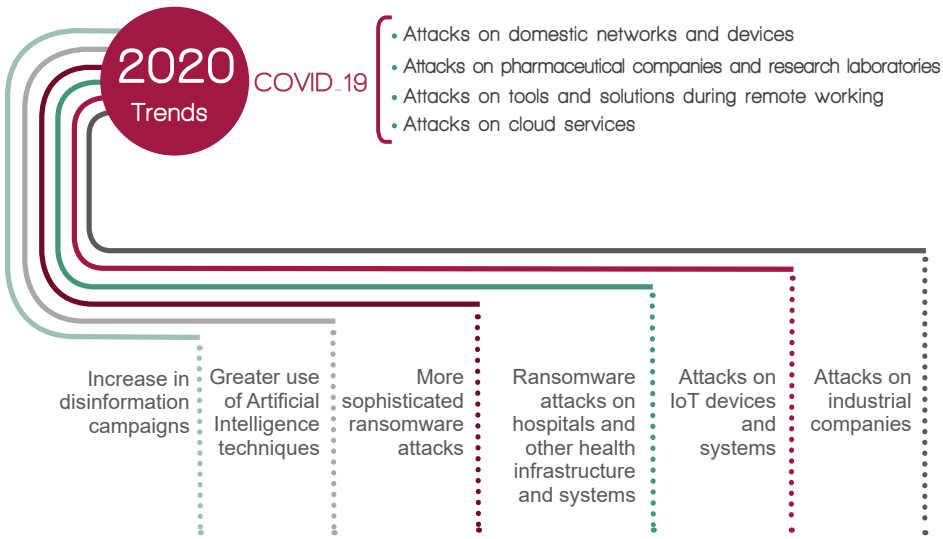


Source: *IBM Security, Cost of a Data Breach Report 2021, except where another source is specified in the text.*

At a glance

- With the pandemic, cyber attacks have increased fourfold and ransomware attacks fivefold.
- 23% of large Spanish companies suffered some type of cyber incident in 2020.
- It is estimated that it takes an average of 280 days to detect a cyberattack.
- Staff training and awareness are key to mitigating cyber security risks

2020: the year of COVID-19 and cyber security

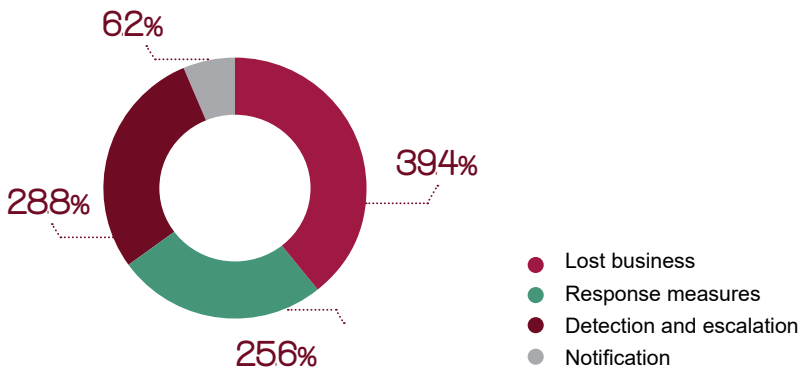


Source: *National Cryptologic Center (CCN)*

At a glance

- The greatest cost (40%) of a cyber attack is lost business
- Regulation requires companies to analyze and monitor cyber risks in the supply chain
- Testing for resistance to cyber incidents is the most effective way to mitigate risk
- Demand for cyber insurance has soared to around US$55 billion

Cyber attacks: the greatest cost corresponds to lost business (% of the total)

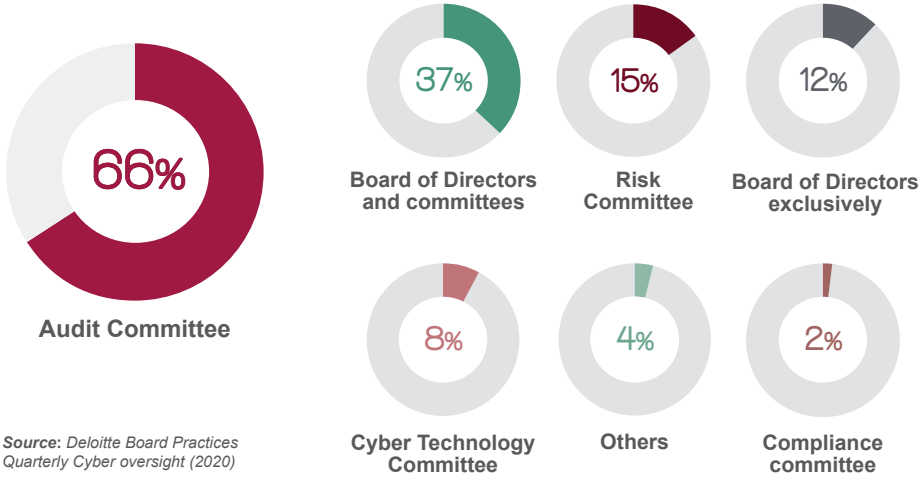


Source: *IBM Security, Cost of a Data Breach Report 2021*

At a glance

- Cyber security must be integrated into strategy and aligned with business objectives.
- The need to appoint a cyber security expert or a specific committee at board level should be questioned.
- The board is briefed primarily on vulnerabilities and trends once a year: Is this sufficient?
- If DORA works effectively in the financial sector, the EU will create sector-specific cyber security rules.

Who oversees cyber security risk?



Source: Deloitte Board Practices Quarterly Cyber oversight (2020)

Connectivity and cyber security

The pandemic accelerated digitization. The increased connectivity among people (remote working) and machines (IoT) has quadrupled cyber attacks. Risk has to be prevented, managed and mitigated before, during and after, in order to be prepared.

This was already a relevant risk and has become a priority due with increased digitization. It is the primary risk highlighted by internal auditors in the Risk in Focus 2021 report[1] and is among the top 10 risks in the 2021 World Economic Forum, which highlights growing digital inequality and the risk of a global breakdown of key internet infrastructure, for which attempts have already been made[3].

With the pandemic and accelerated digitization, cyber security risk has exceeded its own boundaries, moving beyond the perimeter to which it was traditionally confined. It has moved on from a physical location (IT infrastructure in the office) to one that is ubiquitous (the cloud allows connectivity from anywhere), whose growth has skyrocketed due to mass remote working. There are now three fronts that need to be controlled and protected: users, access and information, all of which lie in a new (distributed) environment where the traditional approach is not enough.

[1] ***Institute of Internal Auditors.*** *2021 Risk in Focus (2020)*

[2] ***World Economic Forum (WEF).*** *2021 Global Risks Report. (2021)*

[3] ***El País.*** *The global crash of thousands of websites alerts to the fragility of the Internet (9 June 2021). Websites of companies such as Amazon, Twitch, New York Times, HBO Max, Hulu, the UK government website, Spotify, and Reddit were down or had access problems for more than an hour.*

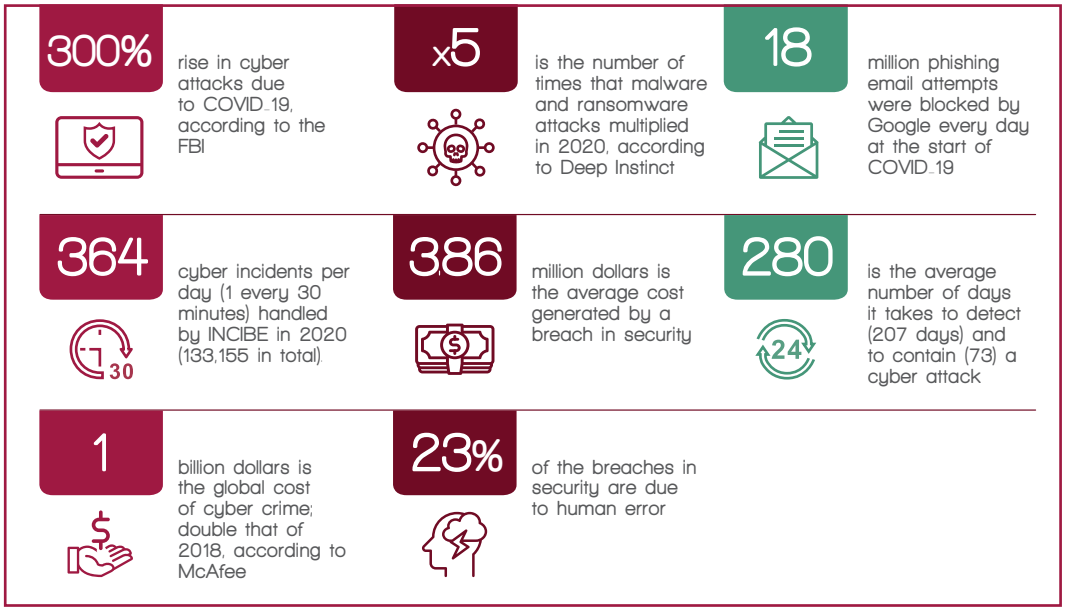
Top 10 challenges according to ENISA

1. Systemic nature. Cyber security risk spreads quickly and widely. It is difficult to assess and mitigate.
2. Preventive technology. The use of Artificial Intelligence in cyber attacks will make detection much more difficult.
3. Unintentional errors. On the increase due to the growing use of connected devices and systems.
4. Supply chain. Hackers exploit any weakness in business ecosystems, whether partners, suppliers or otherwise.
5. Automation. Data analytics and Artificial Intelligence will help in the design of more robust cyber security strategies.
6. False positives. Reducing them is key to optimizing efforts and eliminating unnecessary alarms.
7. Zero-Trust model. Users, devices and applications must be verified for every request for access to a corporate resource[4]. For many, the Zero-Trust model is the key to future security.
8. Migration to the cloud. A cloud configuration failure can leave data exposed. Systems are being designed that automatically identify these errors.
9. Hybrid threats. They combine the digital and physical worlds to appear more real. Disinformation and fake news are serious dangers.
10. The cloud as a target. Increasing reliance on cloud infrastructure will increase attacks, not only on companies that use them, but also on service providers.

Source: *European Union Cybersecurity Agency (ENISA). Threat Landscape: The year in review (2020)*

[4] ***2021 Hacker World.*** *Presentation on Zero Trust by Asier Ortega Peciña, Senior Sales Engineer at Forcepoint Iberia.*

The risk of cyber security in data.



Source: *IBM Security, Cost of a Data Breach Report 2021, except where a different source is specified in the text.*

EU sets the tone: regulations on the move

In 2018, the EU took an international stance on security and data protection with the General Data Protection Regulation (GDPR). It now has a series of cyber regulations in place[5], starting with its physical and digital security strategy and continuing with the NIS 2 Directive for sensitive sectors, the Resilience Directive, the digital identification regulation (eIDAS2) and the Digital Operational Resilience Act for the financial industry, better known as DORA. The EU's approach is to act on the three key fronts: technology, processes and people.

[5] *Data collected by* **Mckinsey** *Cyber security in Iberia: Aligning business and the board (April 2021).*

Ransomware attacks

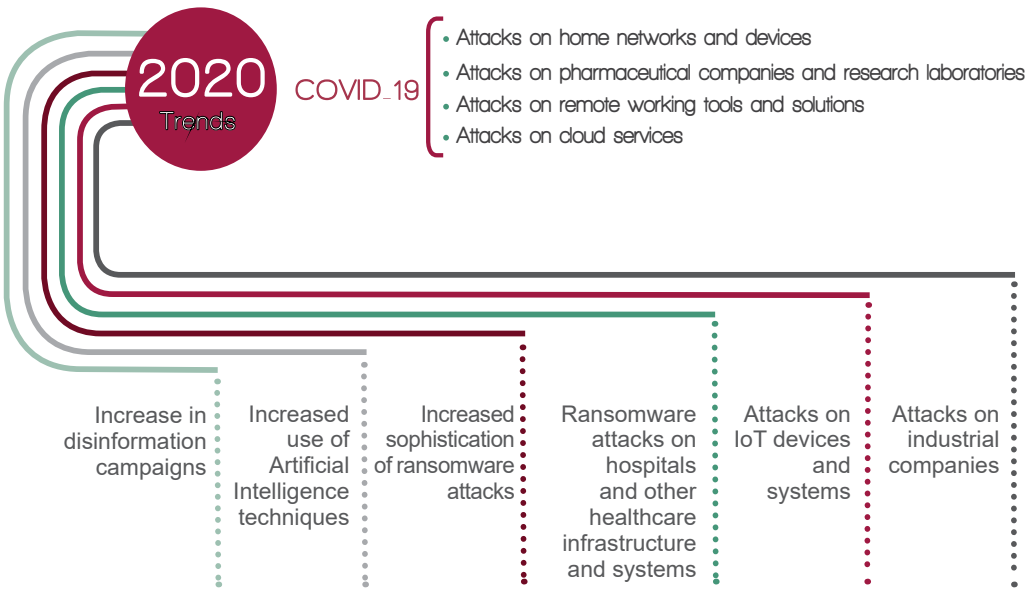
Cyber attacks have quadrupled since the start of COVID-19, according to FBI data. Ransomware attacks, such as WannaCry (2017), for which a ransom is demanded to unlock the hacked data, have increased fivefold. They are increasingly sophisticated and attack sensitive sectors or so-called critical infrastructure. Hospitals and pharmaceutical companies are under heavy attack.

INCIBE handled a total of 133,155 cyber incidents in Spain in 2020, which equates to 364 per day, i.e. one every 25/30 minutes.

Data from the National Cryptologic Center (CCN) reveals that 23% of large Spanish companies suffered some type of cyber incident in 2020, a percentage that falls to 12% for SMEs, which are less digitalized, and rises to 28% for citizens[6]. Nothing like that had ever been seen before.

The question is no longer whether a company will suffer a cyber attack, but when. Cyber crime has become more professional and several new state-sponsored players have emerged.

2020: the year of COVID-19 and cyber security



Source: *National Cryptologic Center (CCN)*

[6] *Data collected by* **Mckinsey** *Cybersecurity in Iberia: Aligning business and the board (April 2021)*

From IT to strategy

From a business perspective, cyber security is experiencing a complete paradigm shift. It has gone from being an IT problem to a strategic issue that involves the entire organization and, if not properly managed, can have a serious economic, regulatory and reputational impact and even lead to the closure of the company[7]. Cyber security cannot be dealt with in a reactive manner; instead, this should be done proactively by anticipating situations.

Users, access and information have to be protected in an environment where a classical approach is inadequate.

Due to the pandemic, the cyber security risk has exceeded its own limits.

The cyber security map

Main risks

- Monetary fraud
- Information theft
- Unavailability of services
- Infrastructure sabotage
- Loss of reputation

Main threats

- To information
- To ICT infrastructure

Profile of the attackers

- Hacking
- Cybercrime
- Hacktivism
- Cyber espionage and cyber terrorism
- Insider

Main attack techniques

- Social engineering
- Fingerprinting
- Enumeration and scanning
- Zero-day (0-Day) attacks
- Spam and Phishing
- Hijacking
- Denial of Services (DoS)
- SQL Injection
- Cross-site scripting (XSS)
- Viruses, malware, worms and Trojans
- Botnets
- Rootkits
- Ransomware
- APT (Advanced Persistent Threat)

Source: *La Fábrica del Pensamiento*
Cyber security: A monitoring guide.

[7] ***El País.*** *Cyber attacks that kill businesses. (2020)*

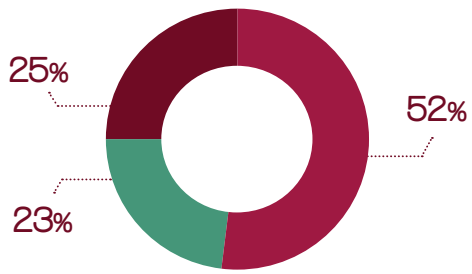
Board responsibility

Regulators and supervisors, who are aware of this growing risk, are asking companies to be prepared. How? By taking different measures. One, by placing responsibility (and requiring technical expertise) at the top: the board of directors and its supporting committees. Two, by introducing severe regulations and sanctions (GDPR is a good example). Three, by demanding business continuity plans and, for the financial sector, by even stress-testing banks, trading platforms and payment clearing and settlement systems[8] Four, by extending the perimeter of control to the supply chain and any other relationship with suppliers or third parties, a historical weak point through which cyber attacks have crept in. And five, by calling for a cyber security governance model and more and better supervision.

The financial industry is being stress tested in order to gauge its cyber resilience

The Audit Committee, as with the Internal Audit, plays a very important role in supervising this risk and ensuring that the organization promotes an adequate cyber security culture.Today more than ever due to remote working, this appropriate culture involves training and raising awareness among the workforce. This is one of the great challenges.

System failures and human error generate half of the breaches (%)



The Audit Commitee must ensure that an adequate cyber security culture is promoted

Source: *IBM Security, Cost of a Data Breach Report 2021*

[8]***European Banking Authority (EBA)*** *EU-wide stress testing (January 2021).* ***European Central Bank (ECB).*** *What is cyber resilience?*

Cyber crime costs $1 billion

Cyber attacks are on the rise and are becoming more and more sophisticated. Cyber crime is not an individual activity, like it was some years ago, but is carried out by organised groups that possess great IT knowledge, different motivations, a business model and even their own R&D&I departments. They are able to get their hands on all kinds of resources, tools and malware from the Dark Web in order to carry out their attacks. There are even forums in which hackers are able to resolve queries and tackle challenges. Cyber crime is considered by many to be Crime as a Service. McAfee says that the global cost of cybercrime now amounts to $1 billion, double what it was in 2018.

It takes an average of 280 days to detect a cyber attack.

Cyber crime has become more professional and even has R&D departments.

DORA opens the door to sector-specific cyber regulations

The Digital Operational Resilience Act, better known as DORA, is a European cyber security regulation that is specific to the financial sector. Take note of that name because there are pre- and post-DORA period,s for this European regulation that will apply directly to all member countries without the need for internal transposition. If DORA is found to work for the financial sector, it will provide a framework that will be replicated by the EU with specific rules for other industries such as energy, water or telecommunications.

[9] **KPMG Trends** *The Cyber crime business model; Key considerations for cyber incident management (2020); Video: Five answers: How to prevent cyber attacks and system crashes (March 2021)*

[10] ***McAfee**: The Hidden Costs of Cyber Crime (2020)*

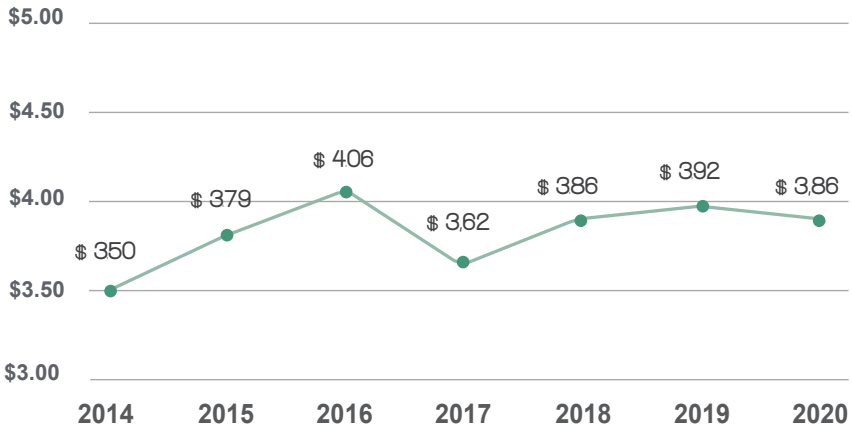
Assessing all impacts

A cyber attack can prove to be highly costly for a company. It can even jeopardize its survival.

In addition to reputational damage, the greatest cost is the loss of business caused by the disappearance of customers or the paralysis of the company itself, as occurs with DoS and ransomware denial-of-service attacks: key operational information is hijacked and a ransom is demanded to free it. These types of cyber attacks have skyrocketed with the pandemic: DoS attacks have doubled and ransomware attacks have increased fivefold, according to IBM data.

Cyber security risk unleashes other associated legal, financial and reputational risks. The greatest impact of a cyber attack comes from the loss of business. There are measures that can help mitigate this, such as business continuity plans, stress tests and cyber insurance.

Average cost per data breach (USD millions)



Source: *IBM Security, Cost of a Data Breach Report 2021*

The weak point: suppliers and partners

Hackers know that suppliers or company partners are a weak link and they try to exploit it. Especially now that any connected device, be it a printer, mobile phone, home automation system or air conditioning system, can be a gateway for hackers. In 2013, a US retailer, Target, suffered a data theft (40 million debti and credit cards) and the hackers' modus operandi was to take advantage of the cooling suppliers connection to enter the systems[11]. According to COSO ERM, 59% of companies have suffered security breaches via a third party[12]. Regulations in place (NIS Directive 2.0, DORA etc) include the obligation to analyze suppliers' cyber security. In mergers and acquisitions, it is also common to include a cyber analysis in due diligence reviews.

[11] ***Reuters.*** *Target cyber breach hits 40 million payment cards at holiday peak (2013)*

[12] ***COSO.*** *Managing Cyber Risk in a Digital Age (2019)*

Legal cost

The legal cost can also be high: it should be remembered that the European GDPR regulation provides for fines of up to 4% of the group's turnover for non-compliance with the obligation to protect personal data. Ongoing European regulations will raise this legal cost.

IBM estimates that the average total cost for a company suffering a data breach is around $3.86 million. But detecting a cyber attack is neither quick nor easy: it takes an average of 280 days, or more than nine months, to detect a cyber attack. More and more companies are investing in cyber intelligence and cyber defense systems that allow them to explore the Deep Web to detect early warning signs that will help them act earlier.

Being properly prepared can later reduce the cost. The chart on the next page shows details of the factors that help mitigate the cost of a cyber-attack, such as incident response testing (ethical hacking is commonly used to detect possible vulnerabilities), business continuity plans and staff training. Even though these issues are important, few companies prepare for them in advance. According to an article in the Harvard Business Review, 47% of organizations have not assessed their preparedness of their cyber incident response teams. This means that the first time they do so will be in the midst of a cyber attack, which is the worst-case scenario[13].

What helps the most in mitigating risk are cyber incident testing and resilience testing.

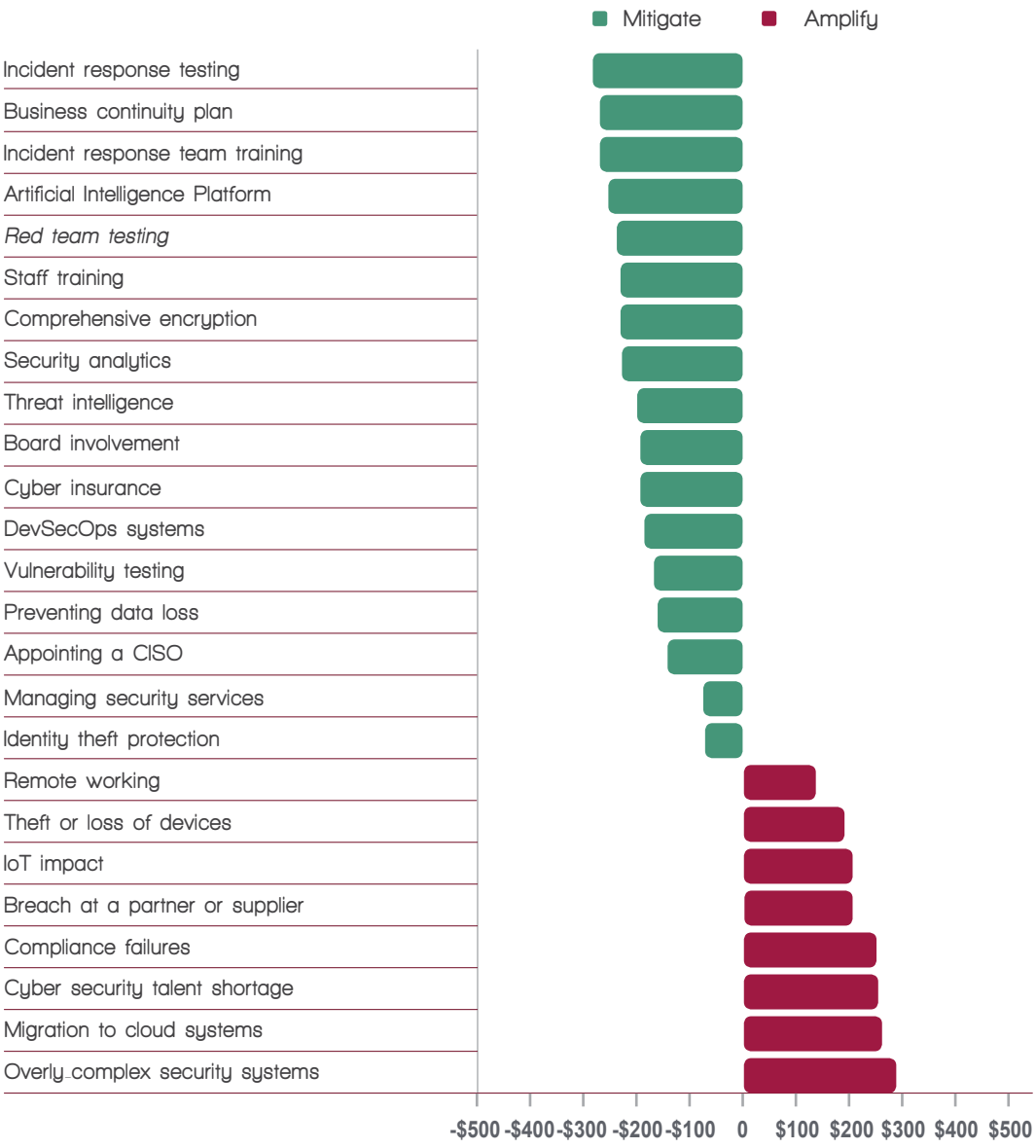
Factors that amplify the cost of a cyber attack include, among others, remote working, due to the vulnerability of remote connection, the theft or loss of corporate electronic devices (laptop, mobile phone, etc.) and errors that occur in the migration to cloud systems.

The greatest cost (40%) of a cyber attack relates to loss of business, that is,... if the company actually survives.

Demand for cyber insurance has skyrocketed to around $55 million.

[13] ***Harvard Business Review.*** *Cyberattacks Are Inevitable. Is Your Company Prepared? (March 2021)*

Factors that mitigate or amplify costs (USD thousands)



Source: *IBM Security, Cost of a Data Breach Report 2021*

Remote working

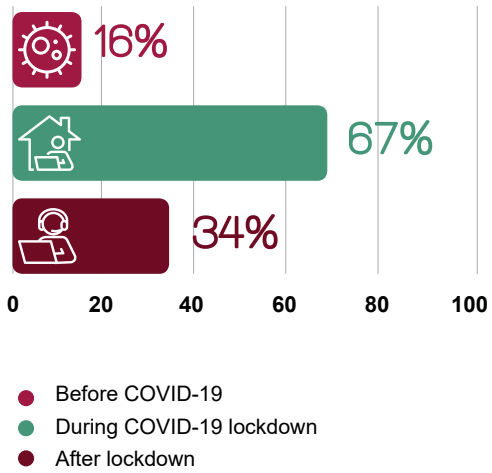
Mass remote working has opened up significant cyber security challenges that must be addressed with tools to control access and with training to raise staff awareness of the following practices, among others: the use of strong passwords and not always the same one; always keeping software up to date; not opening (or clicking on) strange or suspicious emails and links; and using secure VPNs.

The biggest problem comes from using personal devices and networks for corporate use: neither home WiFi nor personal mobile phones have the same levels of cyber security as corporate ones.

For example, a secure corporate mobile phone does not permit the user to download any apps: they remain blocked.

Prior to the pandemic, 47% of European companies surveyed by Cisco[14] had not prepared their systems for this massive amount of remote working, which requires constant videoconferencing and collaborative tools. The result? 93% had to update their cyber security policies, adopting three main measures: increased VPN capacity, implementation of multi-factor authentication (MFA), greater web control and more restrictive policies for use.

European companies with more than 50% of staff working remotely



93% of companies had to upgrade their cyber security due to the onset of the pandemic and the arrival of mass remote working.

Source: *Cisco, Future of Secure Remote Work Report (2021)*

[14] ***Cisco.*** *Future of Secure Remote Work Report (2021) Security Outcomes Study - Proven Factors for Your Security Program (2021) Simplify to Secure Cybersecurity Report (2021)*

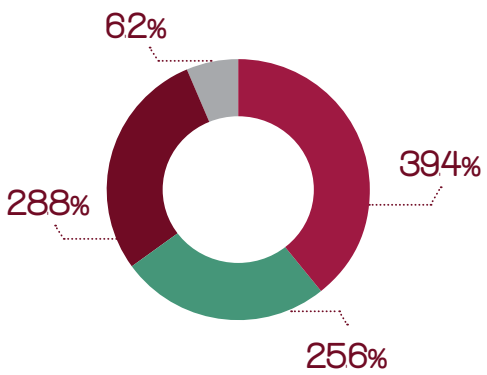
Social engineering

People are the most vulnerable link in the cyber security chain. That is why they are the target of malicious mailings, which appeal directly to human weaknesses. This is known as social engineering, with multiple forms of expression such as phishing and identity theft. At the onset of the pandemic, Google blocked more than 18 million suspected malware or phishing emails every day. CEO fraud, is known as such because the aim of the cyber attack is to impersonate a senior manager (via email) so that employees quickly obey the boss's (false) orders. The aim? To request payments or transfers in order to extract money from the company. It is essential to be very vigilant in detecting and reacting to any suspicious emails and to establish channels for employees who detect them to be able to report them quickly.

Mergers and acquisitions include analysis of cyber security in due diligence reviews.

More and more companies are investing in cyber intelligence in order to detect alerts on the Deep Web.

Cyber attacks: the greatest cost relates to lost business (% of total)

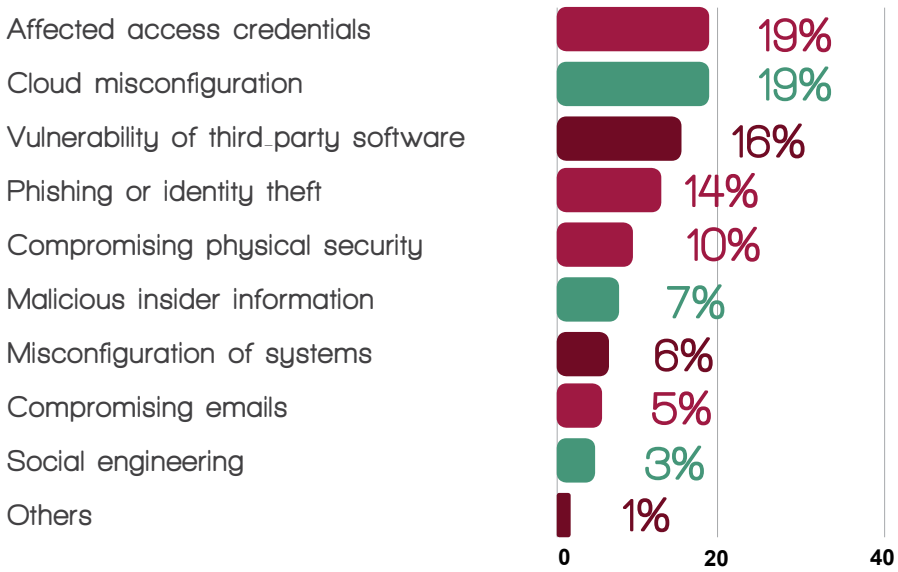


Source: *IBM Security, Cost of a Data Breach Report 2021*

Cyber insurance: pay attention to the extent of coverage

Cyber insurance is becoming an increasingly common practice in companies, especially among larger ones. This is not so much the case for SMEs and the public sector, due to the complexity of these policies. The global cyber insurance market is estimated to be worth $5.5 million in premiums, according to McAfee[15]. Contracts are complex: the fine print and terms and conditions have to be closely studied, and there is a likelihood of having a dispute in court. Of the claims made in 2017 in the US, only 28% were actually paid, at an average amount of $188,525, which is only about a third of the estimated average cost per cyber attack.

Types of malicious attacks by type of threat (Percent of the total)



Source: *IBM Security, Cost of a Data Breach Report 2021*

[15] ***McAfee:*** *The Hidden Costs of Cybercrime (2020)*

Governance framework

Countries are upgrading their national security policies and strategies, ranging from a physical approach for a digital environment, to cyber security strategies. In Spain, the latest revision dates from 2019[16]. What is defined as critical infrastructure receives a special status under a specific regulation and organization: the National Centre for Critical Infrastructure Protection (CNPIC).

Businesses also need to update their control frameworks within the new context. There are a number of existing control frameworks on cyber security in place. Highlighted below are[16] some national and international benchmark institutions that regularly provide warnings, frameworks, trainings, recommendations and good practices.

Countries and companies are adapting their cyber security policies, strategies and frameworks to the digital environment. Advisors need to understand the risk and ensure adequate controls. There are discussions regarding the need to appoint a cyber security expert on the board or a specific committee.

[16] ***IBOE.*** *Order PCI/487/2019 of 26 April on the publishing the 2019 National Cybersecurity Strategy, approved by the National Security Council.*

[17] ***INCIBE; ENISA;*** *National Centre for Critical Infrastructure Protection (CNPIC); National Institute of Standards and Technology (NIST): Cybersecurity Framework (2018) and Cybersecurity Guidelines (March 2021); Centre for Internet Security (CIS); National Cyber Security Centre (NCSC) and Information Systems Audit and Control Association (ISACA). Securities and Exchange Commission (SEC): Commission Statement and Guidance on Public Company Cyber security Disclosures (2018) Cyber security and Resiliency Observations (2020)*

COSO also recently (December 2019) developed new guidance: *Managing Cyber Risk in a Digital Age*. The document underlines the role of the board of directors and its supporting committees, such as the Audit Committee, in overseeing such an important risk. There must be a clear framework, aligned with objectives, strategy, risk appetite and risk tolerance[18].

The COSO ERM framework

Governance and culture	Set strategy and objectives	Performance	Review and correct	Information, communication and reporting
Governance sets the tone for the organization, reinforcing the importance of cyber vigilance and establishing oversight responsibilities.	Cyber security is integrated into business strategy and objectives. An analysis should be made of internal and external factors, their influence on risk, as well as establishing cyber security risk appetite and tolerance. In assessing the program, Internal Audit will analyze the effectiveness of control mechanisms.	Identify, assess and prioritise (depending on likelihood, impact and risk appetite) cyber risks that may affect the achievement of strategy and objectives. Analyze the response and reinforce response measures, business continuity, data security and crisis management, among others.	By reviewing cyber security management practices and capabilities, an organization can gauge strengths, its weaknesses, room for maneuver and impact in the face of a major change in the environment. Specify objectives, KPIs and consequences in case these objectives are not met. Information, communication and reporting.	Implement a reporting process with key data, segmented according to audience, and with the necessary periodicity at various levels to be able to respond adequately to cyber risks. Clearly develop the steps and protocols to be followed and carry out simulations to see how they work.

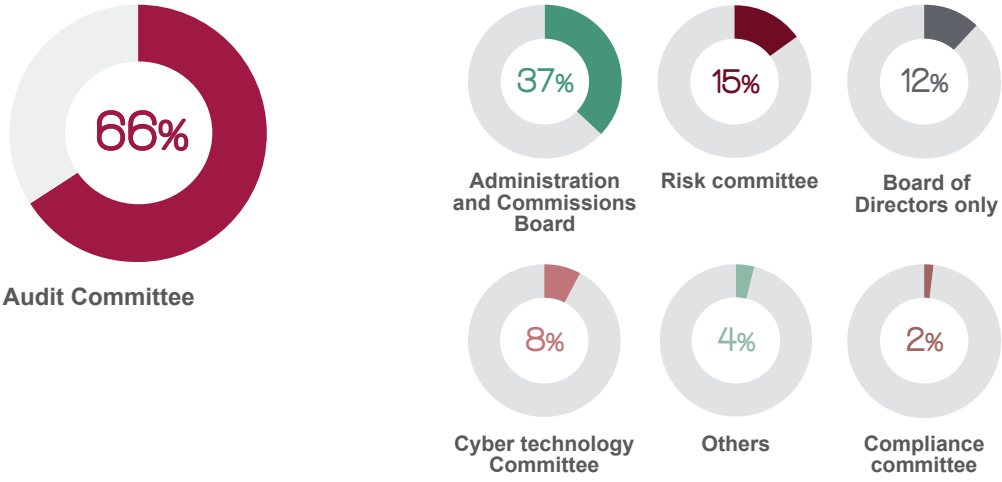
Source: *COSO ERM. Managing Cyber risk in a digital age.*

[18] ***COSO.*** *Managing Cyber Risk in a Digital Age (December 2019)*

SEC: inform about risk supervision

One of the international references available is the SEC's 2018[19] guidance on cyber security disclosure, which specifies multiple aspects, including how and when oversight by the board of directors and its committees should be reported. When? When cyber security risks are significant (i.e. material) to the company's business. How? By stating who deals with cyber security matters with the board (and how), and how the board complies with its duty to oversee this risk and the systems, controls and processes in place. The SEC, like other regulators, requires the board to be vigilant and to understand technology and security issues and how cyber security risks are managed in the organization. There are discussions regarding the need to appoint a specific cyber security expert or committee at board level.

Who supervises cyber security risk



Source: *Deloitte Board Practices Quarterly Cyber oversight (2020)*

[19] ***Securities and Exchange Commission (SEC):*** *Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018) Cybersecurity and Resiliency Observations (2020)*

Board members do not need to be computer engineers, but they should know and understand cyber security risk. Some companies are assigning a cyber security expert to the board. That is the debate going on right now. Other companies are creating a specific cyber security committee: although this segment barely represents 10% internationally, Gartner believes it will be 40% by 2025[20].

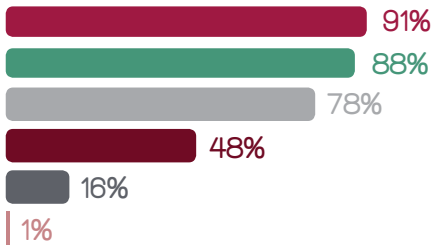
With the increasing value of data, all sectors are susceptible to attack. Cyber security should be on the agenda when starting any project, product or service, from the very beginning.

The board and committees are informed of vulnerabilities and trends once a year: Is this enough?

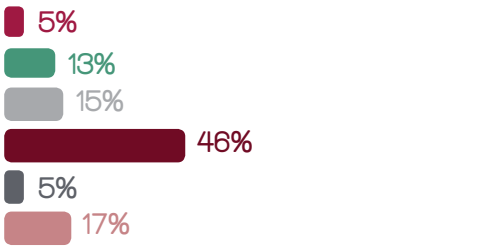
Gartner: 40% of large companies will have a cyber security committee by 2025 (currently 10%)

Cyber security information reaches the board and its committees

What are they informed about



When they are informed



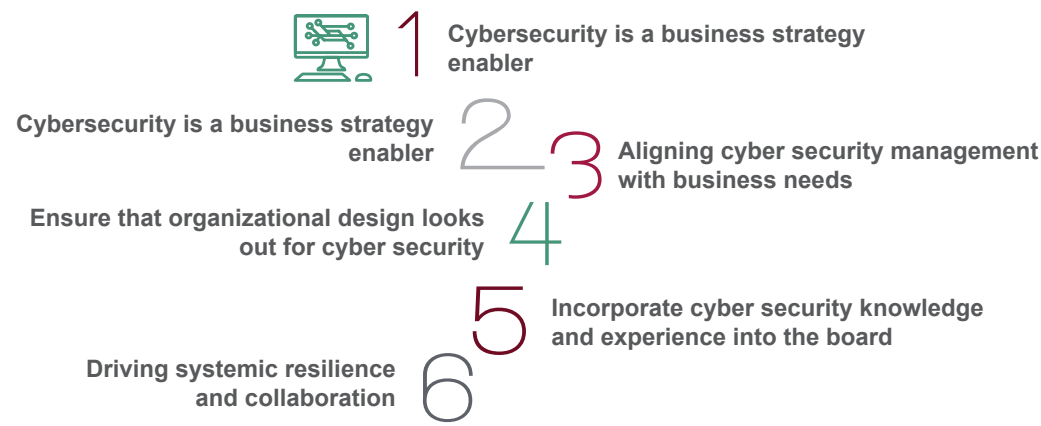
Source: *Deloitte Board Practices Quarterly Cyber oversight (2020)*

[20] ***Gartner:*** *Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025 (Enero 2021)*

Attacks on critical infrastructures and essential services

Cyber attacks on critical infrastructures or essential services are becoming evermore frequent[21]. Since the start of the pandemic, oil and gas installations (United States, Saudi Arabia and Taiwan), electricity grids (India), sanitation (Israel), government agencies (Australia, Spain (SEPE), universities (Oxford), hospitals (Germany, France, United Kingdom, Ireland, Spain), central banks and stock exchanges (New Zealand) have all been attacked. The list is growing[22], which has led US President Joe Biden[23] to expand the list of essential sectors. Europe has done the same with the NIS 2.0 Directive, which also underlines the obligation to monitor supply chain cyber security. It is all part of the new EU Cyber Security Strategy[24].

Six principles for a cyber-resilient organization



Source: *World Economic Forum (WEF), National Association of Corporate Directors (NACD) AND Internet Security Alliance (ISA): Principles for Board Governance of Cyber Risk (March 2021)*

[21] ***Deloitte.*** *The impact of Cyber on "critical infrastructure" in the Next Normal (2020)*

[22] ***Reuters.*** *Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed (9 mayo 2021)*

[23] ***Reuters.*** *Biden administration eyes cybersecurity funding after hacks (18 May 2021)*

[24] **European Commission**. *New EU Cybersecurity Strategy and new rules to increase the resilience of physical and digital critical entities.*

Six key recommendations for board members

Finally, here is a summary of the six key principles and recommendations for becoming a cyber-resilient organization, with appropriate governance and board oversight of cyber security, as recently outlined by the World Economic Forum (WEF) in a report produced in collaboration with the National Association of Corporate Directors (NACD) and the Internet Security Alliance (ISA)[25].

1. **Never take off your cyber security glasses.** Cybersecurity must be on the board's strategy and agenda. It requires committed leadership and a cyber security culture. Everything needs to be looked at without taking off your cyber security glasses: innovation, digital transformation, business strategy, mergers and acquisitions, product development, business expansion, etc.

2. **Appetite, indicators, governance framework**. Cyber security risk needs to be measured against strategic, regulatory, legal and business objectives. Determine and review cyber risk appetite and tolerance level, establish cyber scenarios, indicators (KPIs) and a robust governance framework, with sound quantification models.

3. **Security profile aligned with business needs.** Good governance requires an alignment between cyber security management and business objectives. All decision-making requires an analysis of cyber risk: e.g., a new product or an app. Good cyber risk management opens up opportunities and mitigates risks.

4. **Security by Design or, from the outset.** Security is part of a company's development process: security analysis should not be left for later, but should be considered from the very beginning, when the product design starts. The organizational structure should be reviewed in order to ensure that the cyber security function is present throughout the company, groups, areas and leaders.

5. **Knowledge and experience.** Directors should directly or indirectly - with the help of senior management, Internal Audit and external experts - ensure that they have the up-to-date knowledge required to adequately monitor this complex and technical risk. In addition to regular audits, it is advisable to review trends, vulnerabilities and noteworthy cyber-incidents. As mentioned above, there is a debate as to whether there should be an expert responsible for cyber security or a specific committee at board level.

6. **Collaboration in order to gain in cyber resilience.** Cyber security risk spreads like wildfire in an interconnected world. Managing it adequately demands high levels of internal and external collaboration. Internally, between different business departments, including suppliers. Externally, within its own as well as other industries, considering public-private collaboration.

[25] *Recommendations put forward in the recent report compiled by the World Economic Forum (WEF), la National Association of Corporate Directors (NACD) and Internet Security Alliance (ISA).*

Cyber security as a competitive advantage.

Cyber security, once confined to the IT department, has become a key cross-cutting element in any organization. Properly managed, it is a driver of business growth. Digital trust generates customer loyalty and more revenue.

Properly managed, cyber security risk can become a company's competitive advantage. Customers are becoming increasingly vigilant with respect to their data security. And they do not hesitate to pull out if something looks suspicious. Conversely, digital trust builds loyalty and enables more and new revenue.

Proper management and oversight of cyber security protects the business from cyber risk while boosting brand trust. A difficult balance must be struck between security and customer experience, managing customer privacy and access, without placing too many barriers or frictions[26]. Training and nurturing internal customers (employees) quickly results in an improved perception and satisfaction by external customers.

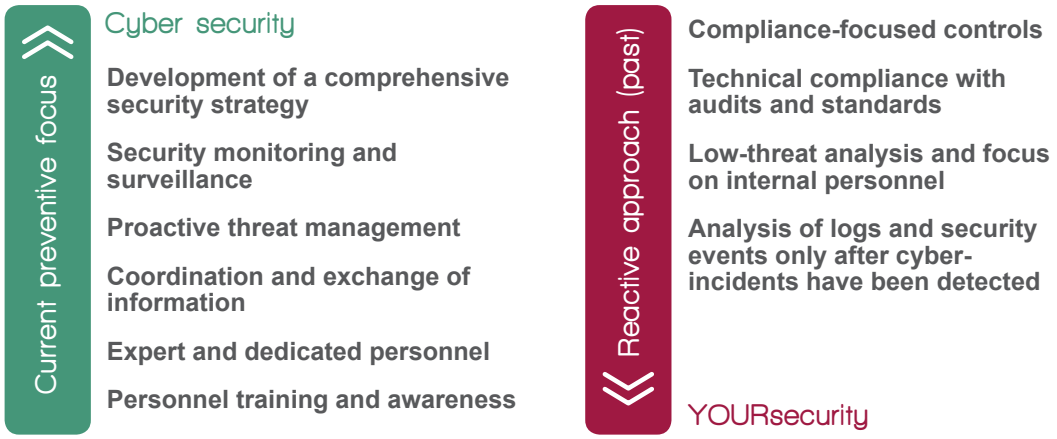
[26] ***Mckinsey.*** *Building security into the customer experience (2020)*

Growth driver

The key is to understand cyber security as an enabler of strategy. Only with robust cyber security can growth be addressed. This vision must start from the top: from the CEO, who will integrate cyber security into strategy and business objectives. This allows alignment of short- and long-term strategies, adding value for business proposals by using cyber security as a differentiator, and leverages on leadership to build a strong cyber culture, as Mckinsey stresses.

This vision is closely linked with the change in approach to cyber security in recent years: from a reactive to a proactive approach, to anticipate and be prepared. New technologies such as Data Analytics and Artificial Intelligence make it possible to further refine this preventive approach, while still offering a personalized service to millions of customers, improving their experience and generating new products and more revenue. Business leaders widely believe that cyber security will further facilitate business innovation, according to a survey in the Wall Street Journal Intelligence and Forcepoint report, which found that 41% of business leaders believe cyber security provides competitive advantage.

A remarkable shift in approach



Source: *La Fábrica de Pensamiento. Cyber security A supervisory guide.*

[27] ***Mckinsey.*** *Transition to the next normal: Enhancing cybersecurity in the Iberian Peninsula. (July 2020)*

[28] ***Wall Street Journal Intelligence and Forcepoint.*** *The C-Suite Report: Business and Security Strategies for Today's Unbound Enterprise. (May 2021)*

Many companies are thinking of adopting new security architecture such as *Zero Trust and Secure Access Service Edge (SASE)*. Take note of this: although may sound technical, cyber security engineers see its adoption as a key step in meeting the challenges of digital transformation, perimeter computing and employee ubiquity.

Cyber security is a key cross-cutting element within any organization.

Bolstering the CISO: the team as the first defence

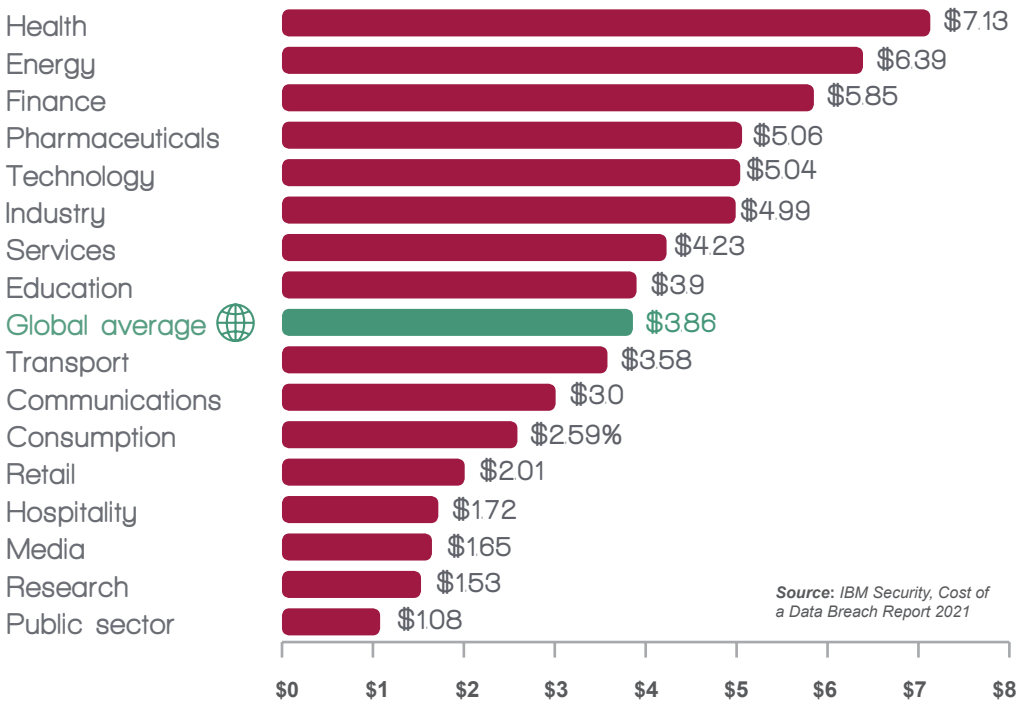
This role is known as CISO (*Chief Information Security Officer*) All companies must have one, in compliance with the Royal Decree approved by the government in January[29]. The Digital Security Officer shall be responsible for drawing up and supervising security policies as well as technical and organizational measures to be implemented in the organisation. Apart from the anecdotal detail of the acronym, the fact is that having a quality technical team is the organisations first line of defense in terms of cyber security. The second line would be an important risk management and the third, without a doubt, would be Internal Audit, which has become evermore relevant regarding this risk.

Digital trust builds customer loyalty and generates greater revenue.

Customers demand security and transparency: they are driven away if they perceive risks.

[29] **BOE.** *Royal Decree 43/2021, of 26 January, implementing Royal Decree 12/2018, of 7 September, on the security of networks and information systems.*

Most affected sectors
(average cost per security breach in USD millions)



Source: *IBM Security, Cost of a Data Breach Report 2021*

Impact on ratings

Cyber security is not traded on the stock markets, but it is present in asset prices via the organization's credit rating. Rating agencies are taking into account the profile, cyber security governance and measures taken by companies before assigning them a rating. Poor management of a cyber attack can lead to a drop in the rating cut, as happened to American company, SolarWinds, *hacked* in 2020[30]. And with a poorer rating, everything becomes more expensive, starting with financing. A multitude of agencies are also emerging that rate security *(security score)* after analysing the ability to protect data from possible cyber attacks. These agencies include *Black Kite, BitSight and SecurityScorecard* most of which are US-based.

Internal Auditor's perspective

Key questions

These are the most relevant issues that, in the eyes of the Internal Auditor, need to be addressed in order to ensure proper prioritization and overseeing of cyber security risk.

1. Has staff training and awareness been stepped up with the pandemic?
2. Are the necessary resources in place for cyber security monitoring, surveillance and preventive management?
3. Are security incident management, response and recovery procedures and protocols in place? Have drills been conducted?
4. Are regular system intrusion (ethical hacking) exercises being carried out?
5. Are cyber security checks carried out on external suppliers before and during the business relationship?
6. Is there an adequate cyber security culture and is collaboration between cyber security and related areas such as compliance, privacy, etc., encouraged?

Internal Auditor Functions

Internal Audit provides assurance in assessing the effectiveness of IT governance, risk management and internal IT controls.

Internal Audit should be involved in or informed of the systems security areas' activities on a timely basis. It can participate in technical security review exercises in order to identify risks not identified in previous layers. An outline is made of the main cyber security issues that should be of concern and subject to review by Internal Audit.

1. Collaborate with the company's management in the creation and development of a cyber security strategy and policy.

to increase the board's awareness of cyber security risks, as well as its involvement and commitment to key cyber security issues, such as updating the company's cyber security strategy.

2. Ensure that the organization has the correct level of maturity and capability for the identification and mitigation of cyber security risks.

5. Integration into the plan. Cyber security is formally covered and integrated into the Internal Audit Plan.

3. Verify the mechanisms for recognizing cyber security incidents originating from an employee or external provider.

6. Understand and develop a company's cyber security risk profile, taking into account new technologies and emerging trends.

4. Make the most of relationships with the company's management

7. Assess
the company's cyber security programme against the NIST cyber security framework, and other standards such as ISO 27001 and 27002.

8. Identify
and assess preventive cyber security control capabilities in terms of user education, training and awareness, as well as digital monitoring and surveillance processes and tools.

9. Ensure
that the monitoring and management of cyber incidents is considered a priority in the company, and that there is a clear escalation process in this regard.

10. Identify
any lacking or shortages in IT and Internal Audit staff that may represent an impediment to achieving the company's cyber security objectives and challenges.

References: relevant regulations and documents.

- Institute of Internal Auditors of Spain. La Fábrica de Pensamiento. Cyber security. A supervisory guide. Directors' Edition; Risk in Focus 2021 Report; Practical Guide on Cyber Security and Data Protection. Mondays at the Institute. Cyber security: European regulation and the role of the Internal Audit 2021 Risk in Focus (2020)
- **Global Institute of Internal Auditors.** The IIA cyber security Resource Exchange. IIA UK-Mind the Gap: Cyber security Risk in the new normal. 2021 Risk Report (2020)
- **National Institute of Standards and Technology (NIST).** Cybersecurity Framework.
- **COSO.** Managing Cyber Risk in a Digital Age (2019)
- **Securities and Exchange Commission (SEC):** Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018). Cybersecurity and Resiliency Observations (2020)
- **Central European Bank (CEB).** Cyber resilience
- **Basilea International Payments Bank (BIS). Covid-19 and cyber risk in the financial sector** (2021)
- **European Commision.** New EU Cybersecurity Strategy and new rules to increase the resilience of physical and digital critical entities.; EU Security Union Strategy 2020-2025; Directive on Security of Network and Information Systems (NIS 2); Critical Entity Resilience Directive and Digital Operational Resilience Act.
- **World Bank.** Financial Sector's Cyber Security: A Regulatory Digest (May 2019)
- **CCN-CERT. Report on Cyber Threats and Trends** (2020)
- **ONTSI.** Dossier of Indicators on Cyber Security and Digital Confidence in Spain and Europe(2020)
- European Union Agency for Cyber Security (ENISA): Cyber Security Incident Report and Analysis System (2020); Threat Landscape: The year in review (2020)
- **INCIBE.** Cyber security balance 2020 Handled over 130,000 cyber security incidents during 2020.
- **BOE.** Order PCI/487/2019 of 26 April, publishing the <4653>National Cyber Security Strategy 2019, approved by the National Security Council.
- **World Economic Forum (WEF), National Association of Corporate Directors (NACD) and Internet Security Alliance (ISA):** Principles for Board Governance of Cyber Risk (Marzo 2021)
- **European Banking Authority (EBA).** EU-wide stress testing (Enero 2021)
- **European Central Bank (ECB).** What is cyber resilience?

- **Global S&P.** Low rating of SolarWinds (April 2021) Article by Simon Ashworth, Head of Analytics and Research, Insurance at S&P Global Ratings. The Increasing Credit Relevance of Cybersecurity (2021)
- **World Economic Forum and University of Oxford.** Cybersecurity, emerging technology and systemic Risk (2021)
- **World Economic Forum.** 2021 Global Risks Report.
- **IBM Security.** Cost of a Data Breach Report 2021. IBM X-Force Threat Intelligence Index.
- **McAfee and the Center for Strategic and International Studies (CSIS).** The Hidden Costs of Cyber Crime (2020)
- **Cisco** Future of Secure Remote Work Report (2021) Security Outcomes Study - Proven Factors for Your Security Program (2021) Simplify to Secure Cyber Security Report (2021)
- **Gartner:** Predicts 40% of Boards Will Have a Dedicated Cyber Security Committee by 2025 (January 2021)
- **Harvard Business Review. Cyberattacks Are Inevitable. Is Your Company Prepared?** (2021)
- **BCG.** Ensuring Online Security in a Quantum Future (2021)
- **Forbes.** Cyber Security In The New Normal: Good Enough Is No Longer Enough
- **Cyber Crime Magazine.** 10 Hot Security Ratings Companies To Watch In 2021 (January 2021)
- **Hacker World 2021.** Presentation on Zero Trust by Asier Ortega Peciña, Senior Sales Engineer Forcepoint Iberia.
- **El País.** The global crash of thousands of web pages alerts to the fragility of the Internet (9 June 2021). Cyber attacks that kill companies. (2020)
- **Reuters.** Target cyber breach hits 40 million payment cards at holiday peak (2013) Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed (9 May 2021) Biden administration eyes cyber security funding after hacks (18 May 2021)
- **Wall Street Journal Intelligence and Forcepoint.** The C-Suite Report: Business and Security Strategies for Today's Unbound Enterprise. (May 2021)
- **Mckinsey.** COVID-19 crisis shifts cyber security priorities and budgets (2020). Transition to the next normal: Enhancing cyber security in the Iberian Peninsula (2020). Cyber security: Emerging challenges and solutions for the boards of financial-services companies (2020). Cybersecurity in Iberia: Aligning business and the board (April 2021). Building security into the customer experience (2020)
- **Deloitte.** Board Practices Quarterly: Cyber oversight (May 2021) Impact of COVID-19 on cyber security. The impact of Cyber on "critical infrastructure" in the Next Normal (2020)

- **KPMG.** Five responses: How to avoid cyber attacks and system crashes. The Cyber Crime business model. KPMG Trends The cyber crime business model Key considerations for cyber incident management(2020); Video: Five answers: How to prevent cyber attacks and system crashes(March 2021)
- **PwC.** Cyber Security: how to manage the impact of COVID-19
- **EY.** Technology and information security

Institute of Internal Auditors of Spain.
Santa Cruz de Marcenado, 33 - 28015 Madrid
Tel.: 91 593 23 45 - Fax: 91 593 29 32
www.auditoresinternos.es

Legal Deposit: M-13527-2022

ISBN: 978-84-124893-5-4

Design and layout: Blondas de Papel S.L.

Instituto de Auditores Internos de España

RiesgosClave

esfera consejeros

The Institute of Internal Auditors

If you are a director of an Institute member company and you would like to register in Esfera Consejeros, please apply here.