GlobalData.

Cybersecurity in Europe

SPONSORED BY

TANIUM

Contents

Introduction

The cybersecurity landscape in Europe is as diverse as the 44 countries in it. Their cyber outlook reflects the impact of multiple factors, including varying attitudes towards risk, privacy, and security in each country as well as in key organisations that operate nationally or regionally. This results in different country-specific regulations that vary in terms of scope, requirements, and enforcement.

In addition, the major industries in Europe have unique cybersecurity requirements based on the nature of their operations and the sensitivity of data they handle. The diversity in technology infrastructure and digital maturity levels of industries also influences the complexity and effectiveness of cybersecurity systems, at a time of an increase in the number and complexity of attacks.

This paper will showcase how you can help yourself to prevent these attacks. It outlines the big picture facing European businesses, and considers the regulatory and compliance picture impacting them. It also looks at the evolving cybersecurity landscape, and the implications for businesses.

The paper includes several examples of how organisations have improved their preventive position, and took on their cybersecurity challenges. It sets out the steps they took to gain – or regain - the necessary visibility, control, and planning in place to be able to **a)** prevent, and **b)** react properly and effectively to thwart and be resilient to attacks. Finally, it outlines some recommendations that organisations should follow to help achieve those goals.

ZAC WARREN

CHIEF SECURITY ADVISOR, EMEA, TANIUM

"The cybersecurity landscape in Europe is undeniably complex and diverse, yet I firmly believe there are simple actionable steps organisations can take to bolster their preventive measures and shield themselves from potential attacks. This paper offers valuable insights into key challenges that European businesses are facing and provides real-world examples of how organisations are successfully elevating their cybersecurity defences."

The big picture facing European businesses

Across the world, 2023 has been a challenging year for keeping ahead of cyberattacks. While the trends of both a growing number and also increasing sophistication of cyberattacks are global, there are specific factors impacting the European market.

These include the Russian invasion of Ukraine, that has increased geopolitical tension in the region and mobilised more state-sponsored groups, as well as the need for many established companies and institutions to undergo digital transformations and to manage the transition from legacy systems.

The stark picture is that spending on cybersecurity is increasing, because breaches are costing more, and that means organisations have to take preventive measures to counter them. According to IBM's Cost of a Data Breach Report for 2023, the average cost of a data breach in Europe is $4.67m in Germany, $4.21m in the UK, $4.08m in France, and $3.86m in Italy. Only Canada, the Middle East, and the United States are higher than Germany's cost.

European organisations that have been the victims of high-profile cyberattacks include the Royal Mail (UK), software provider Nebu (The Netherlands), eyewear company Luxottica (Italy), government software provider Xplain (Switzerland), and British Airways, Boots, and the BBC (UK). We are seeing breaches in all industries, from airlines to retail, from banking to manufacturing. And the pace of attacks is increasing.

As a reault, the European cybersecurity market is evolving on the back of the digital transformation trend evident across the region. The European cybersecurity market was worth $33.3 billion in 2022, compared to $156.1 billion globally, according to GlobalData. By 2026, global security revenues will reach $232.1 billion, while Europe alone will be $48.7 billion.

In Europe, managed security services will be the largest segment of the differing products and services in 2026. Revenues will increase by a compound annual growth rate (CAGR) of 8.2% between 2022 and 2026, reaching $20 billion in 2026 (or about 41% of the European market). Identity & access management will be a distant second, with a 9% revenue share, followed by endpoint security platforms. Fraud prevention and transactional security will be the fastest growing segment, expanding at a CAGR of 13% between 2022 and 2026.

The top three industries driving the growth of the cybersecurity market in Europe are manufacturing, information technology (IT), and retail. As the chart below shows, in manufacturing, information technology and retail, as well as insurance, cybersecurity market revenues are increasing. In the UK, cybersecurity revenues in manufacturing are set to rise from $363m in 2022 to $488m in 2026. In retail, the increase will be from $332 to $430m, and in insurance from $221m to $313m. In Germany, cybersecurity revenues in manufacturing will rise from $928m in 2022 to $1.2bn in 2026. In IT, the rise is from $409m to $721m, and in retail from $312m to $445m. Revenues for France, Ireland, The Netherlands, and Spain follow a similar upward trajectory.

Public investment on cybersecurity in the EU has been fragmented and often poorly supported by government-led initiatives. (Please see Compliance section for details of regulatory measures) As cybersecurity investment is dispersed across several budget categories (research and development, defense, digitalisation, IT, etc.), precise figures are hard to estimate, but EU public spending on cybersecurity is between €1 billion and €2 billion annually, according to the European Investment Bank's *European Cybersecurity Investment Platform* report.

Manufacturing, information technology (IT), and retail are the key drivers of cybersecurity in Europe

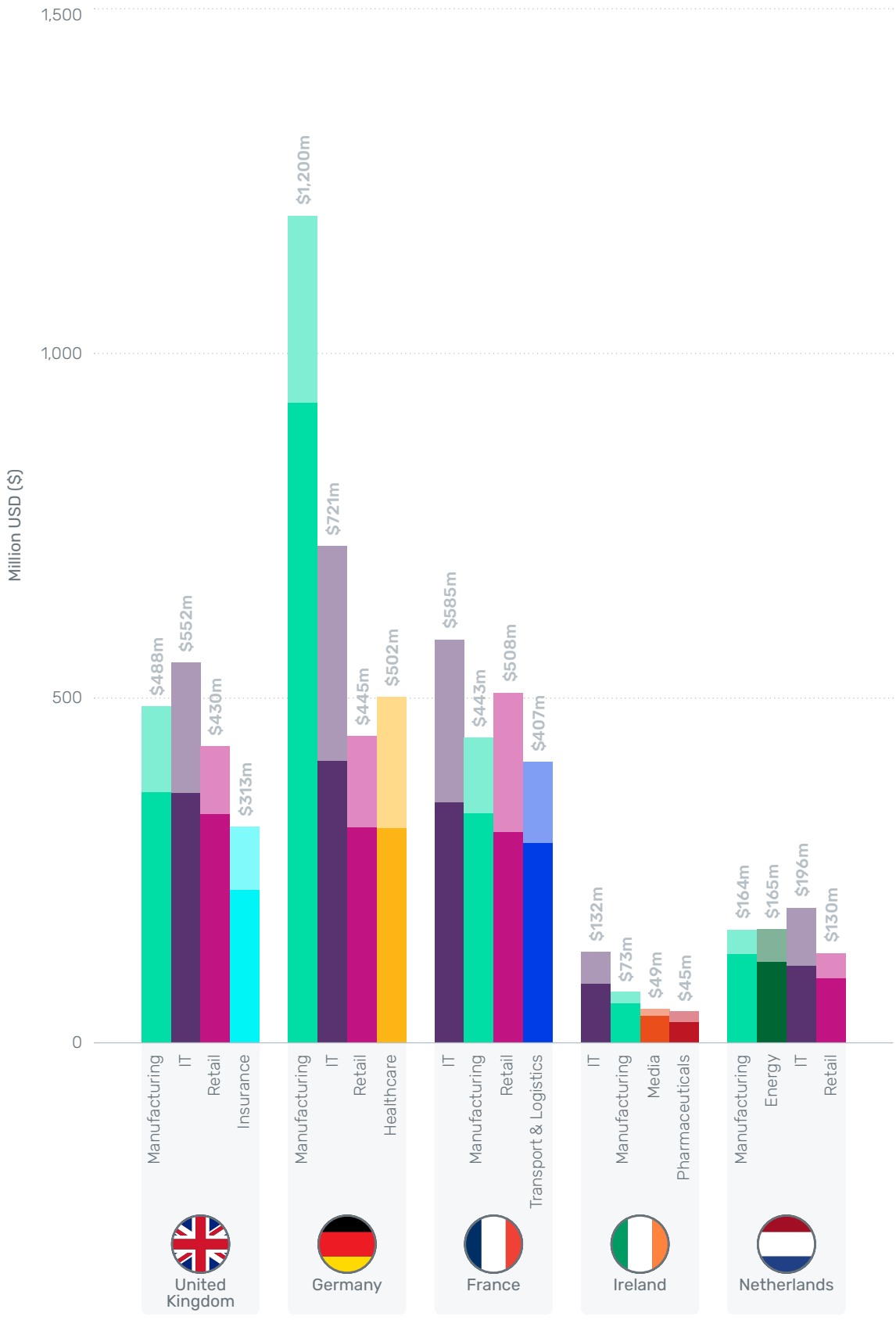
Cybersecurity market revenue in 2022 and 2026 by top five industries in select European countries

Key

Projected values shown for 2026 as USD$

Solid colours = 2022

Tinted colours = 2026



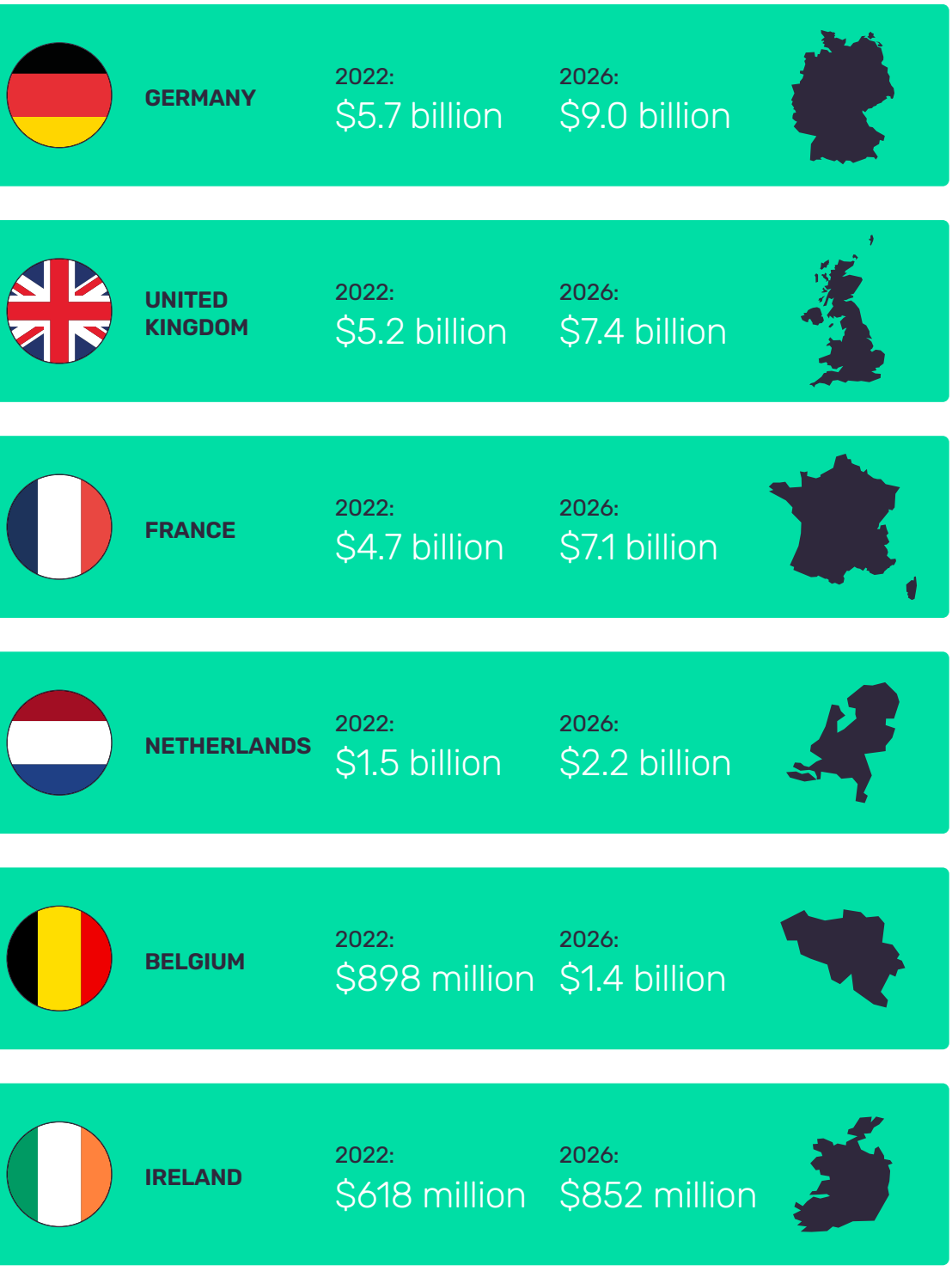
Source:
GlobalData

Note:
The Others segment includes agriculture, arts entertainment, recreation, wholesale, business & professional services, construction & engineering, ICT-related services, miscellaneous services, and real estate, rental and leasing.

Germany and France are expected to maintain their leadership positions in the EU cybersecurity market, followed by Italy, Spain, Poland, and the Netherlands. Additionally, France and Germany spend the most money on cybersecurity in Europe. Prior to Brexit, the UK was the largest EU cybersecurity spender, both in terms of the total volume of investments and in terms of the number of companies, according to the *European Cybersecurity Investment Platform* report.

As the chart below shows, by revenue, Germany, the UK, and France will continue to be the biggest cybersecurity markets in Europe by 2026.

Germany, followed by the UK and France, will lead the European cybersecurity market by 2026



Source: GlobalData

Preventive and resilient, not just responsive

The challenge facing Europe's biggest enterprises is not only in preventing cyberattacks, whether they are delivered through phishing attacks, supply chain hacks, or social engineered targeting, but being resilient enough to recover from them when they happen. Taking steps to defend against a cyberattack will not be guaranteed to prevent one – though it will help – but you can also plan to be as resilient as possible and give yourself the best chance to recover from one.

It helps if, as an organisation, you have cybersecurity investments in place. That is far from always being the case. Too often security practitioners feel their work is ignored or undermined until it is too late. According to a survey in Tanium's 2022 *'Cybersecurity: Prevention is better than the cure'* research study, almost two-thirds of respondents (65 percent) agree that IT and security teams believe an event has to occur before they can receive higher cybersecurity investments.

A common feature of growing organisations is the value they place on trying to be responsive, after an attack. Rather less prominence is given to resilience, a less glamorous quality, which tends to float under the radar until it is needed. The 2022 Tanium analysis showed that it sometimes takes a cyberattack to happen before senior leadership teams sign off greater cybersecurity budget with 77% of organisations who have experienced a cyberattack/data breach in the last 6 months agreeing, 'the leadership in my organisation are only concerned by cybersecurity following a cyber security incident'.

79% **Eight in 10 (79 percent) of professionals surveyed said that more cybersecurity budget is likely to be assigned following a data breach, not ahead of one.** That is shutting the gate after the horse has bolted. The conclusion must be that some senior leaders still do not fully appreciate the preventative role that cybersecurity plays in protecting the business. Without the right toolset in place, an organisation lacks the visibility, control, and planning in place to be able to **a)** prevent an attack, and **b)** react properly to it.

32% **Less than a third (only 32%) of European businesses have a cybersecurity strategy.** The report found that 52% of respondents in Europe reported experiencing some kind of cybersecurity incident in 2022. The incidents cost 32% of European organisations affected at least $500,000 or more. On the brighter side, 81% of European organisations indicated plans to increase their cybersecurity budget by at least 10% over the next 12 months.

<10% **In almost all European countries, less than 10% of companies are deemed sufficently prepared to tackle today's cybersecurity issues.** The UK and Germany are exceptions, with 17% and 11% of companies in a mature state of readiness respectively, according to Cisco's Cybersecurity Readiness Index. Only 9% of European companies have the 'Mature' level of readiness needed to be resilient against cyber risks, says the report. Globally, 15% of companies are at a Mature stage.

While cybersecurity has become a global business issue, customer needs are extremely diverse. For instance, banking, insurance, and financial services, where transactions are primarily digital today, have been investing extensively for a long time to defend their systems. In contrast, the digital revolution in the manufacturing, retail, and healthcare sectors is only getting started. So, in these sectors, vulnerabilities are already being exploited by attackers when security upgrades to legacy systems are not implemented across the value chain.

Recognising these evolving threats, some companies are adopting tools like firewalls and data encryption to protect their IT systems. They are enhancing their expertise to prepare for attacks through crisis simulations and communication plans. In addition, they must strategically focus and invest in tools for early detection and prompt response in order to be resilient against potential cyberattacks.

Compliance and regulation

The increasing frequency and multifaceted nature of cyber threats are challenging the status quo. Any organisation that fails to comply with its industry's specific regulations is at high risk of a cybersecurity breach. Noncompliance to regulations can lead to other consequences, including legal penalties, damage to the company's reputation, and loss of third-party trust. The need for cybersecurity compliance is now being espoused by governments worldwide, including the European Union (EU).

No business can be completely immune to cyberattacks. Most organisations are at risk. The key factor in cybersecurity is how resilient you are to those cyberattacks.

At the country-level, the UK has introduced a mandatory reporting obligation for managed service providers to disclose cybersecurity incidents. It also introduced a minimum security requirement, which could see managed service providers fined GBP17 million ($20 million) for non-compliance.

Please see the EU and national government regulations below and use them as a checklist for compliance.

EU REGULATIONS

A new EU directive, NIS2, sets out tighter cybersecurity obligations regarding risk management, reporting obligations, and information sharing.

The directive was formally adopted in November 2022 and member states have until 17 October 2024 to transpose its measures into national law. The directive will introduce new rules across the EU member states to improve the security of networks and information systems. They must meet stricter supervisory and enforcement measures and harmonise their sanctions. The requirements include incident response, supply chain security, encryption, and vulnerability disclosure, among other provisions. It also establishes a framework for better cooperation and information sharing between authorities and member states and creates a European vulnerability database. The original European cybersecurity directive was set up in 2017, but EU countries implemented it differently, leading to insufficient cybersecurity levels.

CRITICAL NATIONAL INFRASTRUCTURE

Each European country will also have its own critical national infrastructure legislation.

For example, in Germany, critical infrastructures – KRITIS - are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequence. They include information technology and telecommunications.

EU CYBERSECURITY ACTS 2019 AND 2023

The EU Cybersecurity Act 2019 presented a cybersecurity certification framework for ICT products, services and processes for EU countries.

Companies doing business in the EU have to certify their ICT products, processes and services once to gain a certificate recognised across the EU. In April 2023, a proposed amendment was announced which expands the certification scheme to include managed security services covering areas such as incident response, penetration testing, security audits and consultancy. In April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the preparedness, detection and response to cybersecurity incidents across the EU. This included the creation of a European Cybersecurity Shield, and a Cybersecurity Emergency Mechanism.

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

European supervisory authorities have concluded a public consultation on an initial batch of policy products under the Digital Operational Resilience Act (DORA).

The Act aims to ensure a consistent and harmonised legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management. DORA, which entered into force on 16 January 2023 and will apply from 17 January 2025, aims to enhance the digital operational resilience of entities across the EU financial sector and to f harmonise key digital operational resilience requirements for all EU financial entities. It covers areas such as ICT risk management, ICT-related incident management and reporting, digital operational resilience testing, and the management of ICT third-party risk.

ONLINE SAFETY BILL

This bill was proposed in an endeavor to make the internet safer for children.

The aim was to reduce the possibility of children seeing harmful and age-inappropriate content, including online harassment as well as content that glorifies suicide, self-harm, and eating disorders. It requires the ability for people to filter out objectionable content, introduces age verification for porn sites, criminalises fraudulent ads, and requires sites to enforce their terms of service. Companies could be fined up to £18 million (around $22.5 million) or 10% of global revenue and see their services blocked if they do not comply.

NEW MANDATORY REPORT FOR MANAGED SERVICE PROVIDERS (MSPS)

In 2022, the UK introduced a new mandatory reporting obligation for managed service providers (MSPs) to disclose cybersecurity incidents.

The government also introduced a minimum security requirement, which could see MSPs fined GBP17 million ($20 million) for non-compliance.

REPORTING OBLIGATIONS

In April 2023, France introduced a new obligation that all cyberattack victims need to report an attack within 72 hours.

If they fail to do so they could be refused any reimbursement under their cybersecurity insurance policy. The attack needs to be reported to the police and judicial authorities.

NETWORK AND INFORMATION SYSTEMS SECURITY ACT

This act passed in 2018 and imposes strict requirements on operators of essential services and digital service providers.

It ensures that these providers sufficiently prove that they are implementing necessary measures to manage risks and protect their networks and information systems.

EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT (AI ACT)

On 14 June 2023, the European Parliament overwhelmingly voted to adopt the proposed European Union Artificial Intelligence Act (AI Act).

The UK & EU will take different approaches but the core principles will remain regarding a 'risk-based' approach to AI use. It's unclear yet how the legislation will impact the European market but it's certainly one that will have a significant impact through 2024 – certainly one to monitor for the future.

Source:
GlobalData

The evolving cybersecurity landscape

The evolving landscape for cybersecurity is full of both technology and business challenges. Russia's military aggression against the Ukraine reshaped the threat landscape in Europe in 2022 and that has continued in 2023. The conflict has mobilised many hacktivists, cybercriminals, and state-sponsored groups.

The typical methods of cyberattacks in Europe include the following:

Distributed denial of service attacks

These are attacks preventing users of a network or system from accessing relevant information, services, or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. In 2022, threats against availability and ransomware rank the highest among the prime threats, a change from 2021 where ransomware was clearly at the top. July 2022 saw the largest ever recorded attacks against a European customer.

Extortion

Ransomware tactics evolved as companies adapted to attacks by upgrading security protocols and improving their backup and restore processes. Threat actors have now begun weaponizing information resident in files. The first step in multiple extortion techniques was double extortion, in which threat actors exfiltrated files before encrypting them. This increased the likelihood of getting a ransom paid by threatening to leak and sell sensitive information.

Malware

Malware means malicious software designed to damage, disrupt, or gain unauthorised access to a device. Traditionally, examples of malicious code types include viruses, worms, trojan horses or other code-based entities that infect a host. Spyware and some forms of adware are also examples of malicious code. In June 2022 alone, adware trojans were downloaded around 10 million times.

Social engineering threats

These are threats that attempt to exploit a human error or human behaviour to gain access to information or services. Social engineering lures users into opening documents, files or e-mails, visiting websites or granting unauthorised persons access to systems or services. And although these tricks can abuse technology they always rely on a human element to be successful. This threat canvas consists mainly of the following vectors: phishing, spearphishing, whaling, smishing, vishing, business e-mail compromise (BEC), fraud, impersonation and counterfeit. 82% of data breaches involved a human element.

Anti-virus

Cybersecurity products such as antivirus, and host-based and network-based intrusion detection systems can be used and will continue to offer some benefits in detecting malicious code. But their effectiveness may be reduced, as the products may not be updated when running on an unsupported operating system and signatures may not be tuned to detect attacks targeted at obsolete systems.

Supply chain attacks

An attack strategy targeting an organisation through vulnerabilities in its supply chain with the potential to induce cascading effects. A supply chain attack targets the relationship between organisations and their suppliers. An attack is considered to have a supply chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets. SolarWinds was one of the first revelations of this kind of attack and showed the potential impact of supply chain attacks. Supply chain attacks accounted for 17% of intrusions in 2021 compared to less than 1% in 2020. One of the most effective in June 2023 was a supply chain attack that targeted the MOVEit file-transfer program, which impacted close to 600 organizations, including, in Europe, the BBC, British Airways, Boots and Aer Lingus.

Artificial intelligence (AI)

AI has a complex relationship with the ever-evolving landscape of cybersecurity. It can serve both as a formidable threat and a powerful solution. Malicious actors are increasingly using AI to enhance the sophistication and efficiency of cyberattacks, which in turn drives companies to use it to enhance their protection. This highlights the need for cybersecurity experts to continually improve their defenses to keep pace with rapidly evolving, AI-fuelled threats. For example, AI-powered social engineering attacks can manipulate individuals and spread disinformation, exploiting human vulnerabilities at an unprecedented speed and scale. To counter those threats, machine learning algorithms can analyze vast datasets in real time for much faster anomaly and threat detection.

Ransomware attacks

The biggest development in cybercrime in recent years has been the rise of ransomware and more recently, extortion. Ransomware encrypts data on victims' systems until a payment is made. Since IT systems are now ubiquitous, ransomware attacks can be truly devastating for victims and their customers, which is why it remains the most acute cyber threat for European businesses and organisations. With more than 10 terabytes of data stolen monthly, ransomware is one of the biggest cyber threats in the EU, with phishing now identified as the most common initial vector of such attacks. It is believed that up to 60% of affected organisations pay up. Ransomware was one of the prime threats during 2022 and that has continued in 2023, though it now more brutally threatens extortion.

Critical business sectors and infrastructure

Critical sectors such as transport, energy, health and finance, including insurance, have become increasingly dependent on digital technologies to run their core business. While digitalisation provides solutions for many of the challenges Europe is facing, not least during the COVID-19 crisis, it also exposes the economy and society to cyber threats. Critical national infrastructure is under threat, with criminals ready to take advantage of any IT/ Operational Technology (OT) vulnerabilities. In industrial systems, including manufacturing, power, and oil and gas, there is a constant fear of a jump from IT into OT systems. Although it happened in the US, the Colonial Pipeline IT systems attack in May 2021 was a wake-up call for governments and critical national infrastructure organisations worldwide, including in Europe. The hack was the largest publicly disclosed cyber attack against critical infrastructure in the U.S. Fortunately, the pipeline's OT systems that actually move oil were not directly compromised during the attack.

A new approach to defending against cyberattacks – the growth of the zero trust model

A zero trust model provides security against ransomware and cybersecurity threats by assigning the least required access needed to perform specific tasks. Instead of assuming everything behind the corporate firewall is safe, the zero trust model assumes that there is a breach and verifies each request as though it originates from an open network.

Regardless of where the request originates or what resource it accesses, zero trust teaches organisations to "never trust, always verify." Every access request is fully authenticated, authorised, and encrypted before granting access. Zero trust offers a solution that is less likely to be breached, and offers better protection for users and data. By authenticating and authorising every user, device, and application — regardless of location — zero trust minimises the risk of a security breach. But it is not easy to implement.

THE BENEFITS OF CHOOSING A ZERO TRUST ARCHITECTURE

1. Reduces the attack surface and risk of a data breach.
2. Provides granular access control over cloud and container environments.
3. Mitigates the impact and severity of successful attacks, reducing cleanup time and cost.
4. Supports compliance initiatives.

A timeline of attacks

December 2022

THE UK

Royal Mail suffered a ransomware attack which brought its parcels business to a halt. The attackers, the LockBit ransomware gang linked to Russia, demanded a large ransom payment in exchange for the decryption key. It took six weeks before the Royal Mail was able to restart international parcel and letter deliveries.

January 2023

Febuary 2023

THE NETHERLANDS

In March 2023, the personal data of about two million Dutch people was found to have been exposed due to a data leak at some market research agencies that use software from market research software provider Nebu. Data from several organisations, including the Dutch Golf Federation (NGF), customers of carrier NS and provider VodafoneZiggo, was exposed as a result of the data breach.

March 2023

April 2023

ITALY & CHINA

Luxottica, one of the world's leading eyewear companies was targeted in a cyberattack. Luxottica – which owns popular brands including Ray-Ban, Oakley and Costa – has suffered several security incidents in recent years. In August 2020, it was caught up in a data breach affecting more than 800,000 EyeMed and Lenscrafters patients.

May 2023

June 2023

SWITZERLAND

The Swiss government said that operational data might have been stolen in a cyberattack on a technology firm that provides software for several departments. Xplain, a Swiss provider of government software, was the victim of a ransomware attack.

UK & OTHERS

A June 2023 cyberattack caught up British Airways, Boots and the BBC in an attack by the Clop ransomware gang, which exploited a piece of business infrastructure called MOVEit, software used to securely transfer files around internal networks. The European Investment Bank (EIB) was also hit by a cyberattack suspected to have been orchestrated by Russian hackers.

Going forward, the question is who will be next?

How organisations addressed the cybersecurity challenge

CASE STUDY 1:

FRASERS GROUP

One of the key cybersecurity tasks for organisations is improving their cyber hygiene. UK retailer Fraser Group operates hundreds of stores, employs over 25,000 people, and runs both brick-and-mortar and online operations in 25 countries. In Frasers' fiscal 2021 year, its sales topped £3.6 billion (approximately $4.7 billion).

Much of Frasers' growth has come via acquisitions, often of troubled companies. It is a strategy that is ongoing. In early 2022, Frasers Group acquired bankrupt online specialist Studio Retail, adding it to a brand portfolio that now includes Sports Direct, Game and Sofa.com.

All that M&A activity also means merging IT systems, a complex task that includes applying cybersecurity best practices. To oversee this challenge, about a year ago, Frasers created a global group for information security and privacy, and which created Frasers' long list of cybersecurity must-haves. These included new capabilities for penetration testing, vulnerability scanning, and greater endpoint visibility. What Frasers really needed was to improve its cyber hygiene, gain visibility into its vulnerabilities and keep its systems secure. Using a dedicated platform enabled Frasers Group to detail what endpoint vulnerabilities it had and what it needed to do to mitigate them.

CASE STUDY 2:

Organisations should ensure that systems are well maintained and administered throughout their life. The devices and interfaces that are used for administrative purposes are frequently targeted, so should be well protected. Spear phishing remains a common method used to compromise accounts with privileged access. Preventing the use of these for routine activities such as email and web browsing significantly limits the ability for a hacker to compromise key systems.

Take the case of Sodexo Benefits and Rewards Services (BRS), a business unit of Sodexo S.A. that products and services to roughly 36 million consumers and beneficiaries in over 30 countries. Supporting the BRS group's IT is complex. Some of its entities have tiny IT departments, while others boast as many as 200 IT staff. Their skill sets vary widely, too.

One of Sodexo's problems was a lack of visibility across all its IT assets. BRS didn't know how many endpoints it had, meaning it also didn't know if all the endpoints were properly secured. The second was poor IT hygiene practices. Patching was inconsistent, and much of it was done manually. The third was a strong security roadmap that was hard to execute and follow across all 30+ markets, mainly due to inconsistent skills and tools on the field to push the activities forward, particularly in remote work conditions.

To overcome some of those challenges, BRS launched an initiative around asset patching with security and infrastructure groups teaming up to find and build a global patching solution. The main objectives were to regain visibility across all endpoints and support the deployment of Security solutions, which was not an easy challenge with so many employees working from home during the pandemic.

CASE STUDY 3:

Zurich Insurance Group has been in business for 150 years with a global presence in 210 countries and territories and well-known brands including Farmers Insurance. Zurich provides property and casualty (P&C) and life insurance products and services to individuals, small and mid size businesses, and multinational corporations.

But the company's success also attracts cybercriminals. With more than 100,000 digital endpoints in a geographically distributed and highly heterogeneous environment, Zurich must keep those endpoints safe and secure.

Where Zurich needed help was with incident response. If attacked, Zurich can determine what occurred, when and where it happened, which devices were affected, and how attacked endpoints can be isolated, mitigated, and then returned to safe operation.

Previously, Zurich lacked tools that could both provide visibility into endpoints and manage them. Its new (Tanium) solution, means it has those capabilities in a centralised dashboard with a set of tools. Paige Adams, Zurich's global chief security officer and his team now have full visibility into their endpoints and are able to keep Zurich's patching up to date. Zurich estimates the savings at up to 100 resource hours a month, based on the automated patching capabilities Zurich has built on top of Tanium's patch tool.

The business implications of cybersecurity

While cybersecurity has become a global business issue, customer needs are extremely diverse. For instance, banking, insurance, and financial services companies, where transactions are now primarily digital, have been investing extensively for a long time to defend their systems. In contrast, the digital revolution in the manufacturing, retail, and healthcare sectors is only getting started. So, in these sectors, vulnerabilities are already being exploited by attackers when security upgrades to legacy systems are not implemented across the value chain.

Recognising these evolving threats, some companies are adopting tools like firewalls and data encryption to protect their IT systems. They are enhancing their expertise to prepare for attacks through crisis simulations and communication plans. In addition, they must strategically focus and invest in tools for early detection and prompt response in order to be resilient against potential cyberattacks.

A critical problem in cybersecurity is resourcing, especially getting the right security leadership in place.

Finding the human resources: the vital role of the CISO

Chief Information Security Officers (CISOs) are responsible for protecting a company's assets (both physical and digital) from cyberattacks. As their role becomes more vital, CISOs tend to fall into one of three distinct categories (roll-over for more information):

TYPE OF CISO	FOCUS	RESPONSIBILITY	KEY SKILLS
Technical	Hands-on experts in cybersecurity technology	Manage security tools, systems, and technical aspects to protect from cyber threats	Deep technical knowledge and experience in cybersecurity
Business-centric	Bridge the gap between cybersecurity and the organisation's goals	Align security strategies with business objectives, ensuring that security supports growth and compliance	Business acumen, risk management, and effective communication
Risk & compliance	Prioritise risk assessment, management, and regulatory compliance	Identify and mitigate security risks, ensure adherence to regulations, and protect the organisation's reputation	Risk assessment expertise, compliance knowledge, and audit capabilities

However, CISOs are traditionally under-represented on corporate boards. In Europe, Heidrick & Struggles's Board Monitor Europe 2022 report showed that only 5% of seats on boards in 2021 were filled by people with cybersecurity experience of any kind. The increasing frequency and multifaceted nature of cyber threats are challenging the status quo – CISOs are becoming invaluable for board governance.

In a 2023 survey by the World Economic Forum, only 25% of respondents indicated that the most senior cybersecurity executive in their organisation reports directly to the CEO. That said, a key challenge for CISOs is gaining the board's support to enable impactful action. This issue originates from the fact that CISOs often find it difficult to translate technical jargon into business language, such as risk, reputation, and resilience. Exacerbating this is the fact that board executives in many organisations lack the understanding and awareness needed to prioritise cybersecurity.

A Harvard Business Review paper 'Boards Are Having the Wrong Conversations About Cybersecurity' says boards too often focus on protection rather than resilience. In many board meetings, the primary topic is how often the company administers a phishing test and the statistical results. That is the wrong perspective for board oversight. No company can be immune to cyber threats, irrespective of the amount it spends on technologies to prevent attacks. While protecting the assets is critical, planning post-attack recovery is paramount. Every company must assume experiencing a cyberattack and prepare to respond and recover with minimal damage, cost, and reputational impact. The board must view cybersecurity resilience as a key operational parameter, asking the operating teams to design a vision for approaches to respond and recover from an attack.

CORPORATE BOARDS MUST VIEW CYBERSECURITY AS A STRATEGIC IMPERATIVE AND INSIST ON REGULAR UPDATES ON:

1. Technical and organisational risks the business faces from potential cyber breaches
2. The degree of readiness to temper any damage resulting from the identification of a specific risk
3. How quickly will the recovery happen from a breach
4. The supply chain risk from potential cybersecurity incidents
5. How protected are we to not lose a business day

One of the big factors that may see CISOs reconsidering their career in cybersecurity altogether is the fear of what will happen to their professional reputation if their company gets breached. Both CISOs and chief security officers (CSOs) worry about having their name dragged through the mud after a data breach, or even facing criminal charges. For instance, a breach at Uber in late 2022 resulted in CSO Joe Sullivan being sentenced to serve a three-year term of probation and ordered to pay a fine of $50,000 after a jury found him guilty of two felonies, including covering up a data breach involving millions of Uber user records.

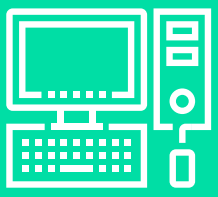
Closing the skills and responsibility gaps

There is a substantial cybersecurity skills gap, with demand significantly outweighing supply. According to GlobalData's job analytics, the average number of open cybersecurity jobs per month globally in 2022 was just under 180,000. The average number of closed cybersecurity jobs per month was significantly less at a little over 60,000, showing the challenge of filling these vacanices. A 2022 survey by the World Economic Forum found that 59% of businesses would struggle to respond to a cyberattack due to the shortage of cybersecurity talent and skills. Cyberattackers exploit skills gap in organisations to extract information. For example, in 2015 the German federal parliament, the Bundestag, was compromised. A skills gap within the Bundestag's cybersecurity team allowed attackers to exploit vulnerabilities in the network infrastructure.

In addition, there are also responsibility gaps, which refer to situations where there is a lack of clear accountability or defined roles among cybersecurity teams. Cybersecurity professionals move from one company to another, creating ambiguity or a lack of consensus on who is responsible, and to what degree, for specific aspects of cybersecurity. This leads to potential gaps in the system. The general lack of cybersecurity staff everywhere compounds the problem.

Addressing it demands developing clear lines of accountability and clearly defined roles, promoting awareness and education among employees, and fostering collaborations among stakeholders, especially third-party vendors. Regulators also have a vital role to play in this. They must enforce robust security frameworks that clarify responsibilities and incentivise compliance, promoting a secure digital ecosystem.

The table below highlights the key complications faced by European businesses related to cybersecurity.



Technology debts

Technology debt refers to the accumulation of outdated or insecure technology systems, software, and infrastructure within an organisation. Outdated operating systems, legacy software, and unsupported hardware can create vulnerabilities that can be exploited by cybercriminals. For example, the 2017 WannaCry ransomware targeted thousands of companies, including healthcare systems in the UK and Spain, that used unpatched Windows XP. In 2020, the SolarWinds attack impacted businesses, including government agencies, in the US and Europe due to delayed software updates and poor security practices. The technology debt hinders the adoption of up-to-date security solutions and hampers an organisation's ability to respond to emerging, sophisticated risks. This exposes critical organisation infrastructure and sensitive data to exploitation. Frequent assessment of operating systems and timely upgrade are paramount importance for business towards cyber-resilience.

Cyber insurance

Cyberattacks are increasing in frequency and severity, so are the costs of both premiums and settling claims. GlobalData's 2022 UK SME Insurance Survey found that 32.7% of UK SMEs felt the level of cyber risk they faced either increased or significantly increased in the year. This is compared to 30.7% in 2021, as concerns continue to rise post-COVID. However, the take up rate for cyber insurance remains extremely low. It was at 12.1% in 2022, up slightly from 11.2% in 2021.

The inflation crisis is a challenge for businesses and the sharp rise in cyber insurance premiums is the key reason that penetration rates are low despite the increased concern around cyberattacks from businesses. Insurers are struggling to convince businesses that a full-scale preventative policy is value for money and there is an ongoing debate over insurers failing to cover nation-state attacks.

Some ransomware gangs are reportedly targeting businesses with cyber insurance policies as they are more likely to pay a ransom. Hence, insurers are re-thinking their cyber policies to mitigate the higher risk of a payout with higher premiums and reduced customer coverage. Cyber insurers are also becoming choosy about the business they support, insisting on reams of information about the security their clients have in place, and excluding some types of incident from the cover they offer. Small enterprises are the prime losers, failing to afford sophisticated security systems and full-scale insurance policies as both concurrently get expensive with the increasing level of risk.

Improving cyberhygiene

Cyberhygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks. It is mandatory, and not a choice, for all organisations.

Europe is a prominent target for cyberattacks due to its economic significance, geopolitical challenges, and abundance of valuable data. These factors make cyberhygiene crucial for all European businesses. Additionally, the General Data Protection Regulation compels companies in EU to emphasis on data protection, making it imperative to prioritise cyberhygiene and comply with rules. Some incidents resulting from lack of cyberhygiene include British Airways' data breach in 2018 that occurred due to airline's website vulnerabilities, and the Colonial Pipeline attack in 2021 that underscored cyberhygiene practices such as updating IT systems, implementing strong access control, and conducting regular backups. The incidents could have been prevented by maintaining secure coding practices and conducting regular assessments, and conducting backups, respectively.

Businesses must make investment commitments and prioritise key areas to ensure cyberhygiene and resilience. Cyberhygiene practices can help in the continuous monitoring of exposure surfaces and to plug security threat endpoints. Security-related communication is of utmost importance in developing a cyberhygience practice to protect the 'crown jewels' (i.e., IT systems and data).

The in-house vs outsourced dilemma

Investing in cybersecurity is a must for all companies, irrespective of their nature of business and size. However, they all face the crucial dilemma of in-house versus outsourced cybersecurity. In-house cybersecurity requires setting up an internal team of cybersecurity professionals to protect the organisation's digital assets, while outsourcing entails relying on third-party or managed security service providers for cybersecurity services.

Both approaches come with specific pro and cons. In-house cybersecurity offers stronger control over security systems as programs can be tailored to meet specific needs, have direct oversight of security operations, and align cybersecurity strategies with their business objectives. However, it requires extensive investment in talent acquisition, training, infrastructure, and maintenance. Big organisations with robust financial and technological resources may choose in-house cybersecurity to maintain control and confidentiality.

In contrast, outsourcing offers access to specialised expertise with all-day, real-time, and advanced security technologies without the need for extensive in-house resources. It can be a cost-effective option for organisations, especially SMEs, that lack the budget or expertise to build an in-house cybersecurity teams. However, it can also introduce concerns about data privacy, vendor reliability, and potential dependencies on external entities.It is vital for organisations to assess the business needs, resources, threat vectors, risk tolerance, and regulatory requirements when deciding between in-house and outsourced cybersecurity.

Recommendations

1

THE INCREASING FREQUENCY AND MULTIFACETED NATURE OF CYBER THREATS ARE CHALLENGING THE STATUS QUO, WHICH IS WHY CHIEF INFORMATION SECURITY OFFICERS (CISOS) ARE BECOMING INVALUABLE FOR BOARD GOVERNANCE.

But they are under-represented on corporate boards in Europe. Only 5% of seats on boards in 2021 were filled by people with cybersecurity experience of any kind. Readers of this paper should ensure they are part of that virtous 5% quota, and not the opposing 95%.

2

PREVENTION IS ALWAYS BETTER THAN CURE.

Research shows that organisations who take a mainly preventative approach to cybersecurity are significantly less likely to have experienced a cyberattack/data breach than those taking a mainly reactive approach. Given how commonplace cyberattacks/data breaches are, the importance of a robust preventative approach to cybersecurity is a key solution to counteract such threats.

3

TOO OFTEN, MORE CYBERSECURITY BUDGET IS LIKELY TO BE ASSIGNED ONLY FOLLOWING A DATA BREACH, NOT AHEAD OF ONE.

That is shutting the gate after the horse has bolted. The conclusion must be that senior leaders still do not fully appreciate the preventative role that cybersecurity plays in protecting the business. Without the right toolset in place, an organisation lacks the visibility, control, and planning in place to be able to **a)** prevent an attack, and **b)** react properly to it.

4

ANY ORGANISATION THAT FAILS TO COMPLY WITH ITS INDUSTRY'S SPECIFIC REGULATIONS IS AT HIGH RISK OF A CYBERSECURITY BREACH.

Noncompliance with regulations can lead to other consequences, including legal penalties, damage to the company's reputation, and loss of third-party trust. The need for cybersecurity compliance is now being espoused by governments worldwide, including the European Union (EU). No business can be completely immune to cyberattacks. The key factor in cybersecurity is how resilient you are to those cyberattacks.

5

A ZERO TRUST MODEL PROVIDES GREATER SECURITY AGAINST RANSOMWARE AND CYBERSECURITY THREATS BY ASSIGNING THE LEAST REQUIRED ACCESS NEEDED TO PERFORM SPECIFIC TASKS.

It provides a solution that is less likely to be breached, and offers better protection for users and data. By authenticating and authorising every user, device, and application zero trust minimises the risk of a security breach.

Sponsor

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Tanium has been named to the Forbes Cloud 100 list for six consecutive years and ranks on Fortune's list of the Best Large Workplaces in Technology. In fact, more than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit www.tanium.com

Follow us on Linkedin: Tanium

Follow us on Twitter: @Tanium

GlobalData.

We are the trusted gold standard intelligence provider to the world's largest industries

We have a proven track record in helping thousands of companies, government organizations, and industry professionals profit from faster, more informed decisions.

Our unique data-driven, human-led, and technology-powered approach creates the trusted, actionable, and forward-looking intelligence you need to predict the future and avoid blind spots.

Leveraging our unique data, expert analysis, and innovative solutions, we give you access to unrivaled capabilities through one platform.

HEAD OFFICE

John Carpenter House
7 Carmelite Street
London
EC4Y 0AN
UK

Tel: +44 20 7936 6400

GlobalDataPlc
GlobalDataPlc
GlobalData.com