VIEIRA DE ALMEIDA

CYBERSECURITY SERIES I

February 2022

CYBERSECURITY SERIES I

CYBERSECURITY – THREATS, CHALLENGES AND ACTIONS FOR 2022

February 2022

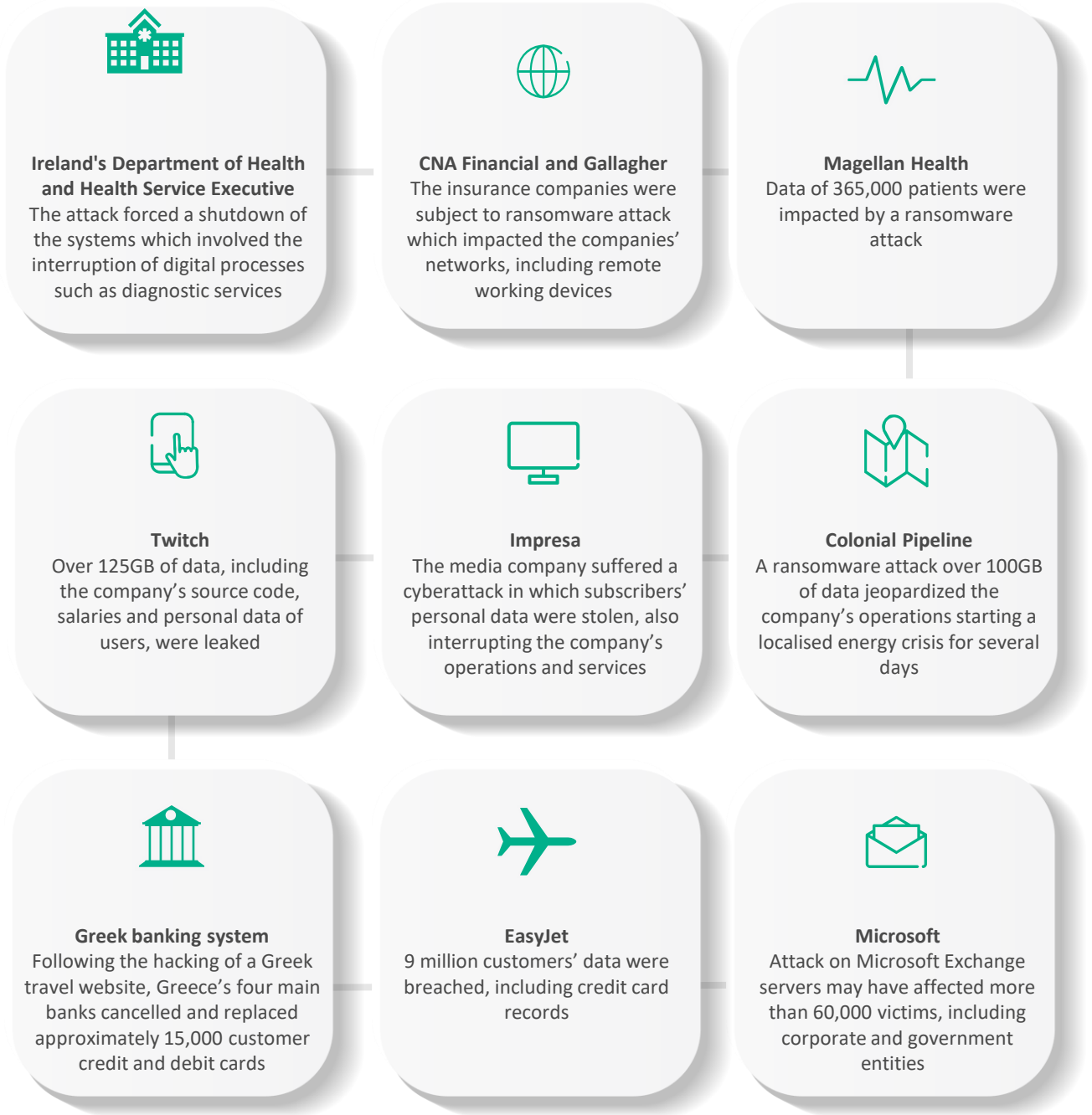
Cybersecurity is increasingly relevant as cyberattacks continue to rise: the transition to the digital economy, together with the impacts of the COVID-19 pandemic, are spurring cyber threats.

The last two years were infamous for high-profile cyberattacks, with malware attacks emerging as the most relevant cyber threat in the EU, and with phishing, identity theft, and ransomware having substantially increased.

The World Economic Forum's Global Risk Report for 2022 has just stressed cybersecurity as a growing risk for industries and organizations.

Therefore it should come as no surprise that cybersecurity has become an increasing focus of intervention by national and European legislators and regulators.

VdA's **Cybersecurity Series** will cover the legal and regulatory issues that organizations should consider and prepare themselves for, in the context of cybersecurity. This first issue sets the scene for what is an inevitable (and indispensable) aspect of an organization's cybersecurity strategy.



THE CHALLENGES

INCREASED DIGITALISATION, AUTOMATION AND CONNECTIVITY SPURRED BY COVID-19 AND 5G/IOT

Changes in working patterns driven by COVID-19 increased cybersecurity vulnerabilities: multiple access points, wider attack surfaces, and home networks (typically less protected) became a central target for cyber-attacks. 52% of legal and compliance leaders are concerned about cyber risks due to remote work. In addition, IoT devices, spurred by 5G, are particularly vulnerable to cyberattacks – it has been predicted that the global number of connected devices will reach 41,6 billion by 2025. The widespread use of AI, machine learning, and cloud services also brings new cyber risks.

INCREASED ATTACKS ESPECIALLY DIRECTED AT PARTICULAR SECTORS

Certain sectors are more susceptible to cybersecurity risks, such as those using sensitive or valuable data. This is the case, for instance, of the health sector (data breaches in the healthcare industry increased by 58% in 2020), the banking and financial sector (including as a result of the increased digitalisation of the sector with payment services, e-money and crypto-assets) and e-commerce (with credit card fraud and fraudulent ID use).

GROWTH OF CERTAIN TYPES OF ATTACKS

Phishing, ransomware, DDoS attacks, privilege access credential abuse and endpoint security attacks are all foreseen to increase. Additionally, attacks on IoT devices and through mobile devices are becoming increasingly frequent, as is state-sponsored cyber warfare.

INCREASED RELIANCE ON THIRD PARTIES

Supply chain security is becoming more and more relevant as companies increasingly rely on third parties, including security service providers and insurers, to perform their activities. The implementation of measures to ensure supply chain security is becoming a legal obligation.

LACK OF CYBERSECURITY EXPERTISE

Implementing cybersecurity policies, incident response frameworks and employee training is increasingly relevant to ensure resilience against cyber-attacks. Indeed, 95% of cybersecurity breaches are caused by human error, and 30% of data breaches involve internal actors.

INCREASED COMPLEXITY OF CYBER CHALLENGES

The tools, techniques and procedures used to execute cyberattacks are increasingly sophisticated and directed (and tailored) at high-profile companies. At the same time, CaaS (cybercrime-as-a-service), such as RaaS (ransomware-as-a-service) models are growing, with attackers being increasingly more distributed and resorting to emerging technologies, including multi-cloud environment and 5G technologies.

THE TRENDS

INCREASED BUDGETS FOR CYBERSECURITY

Both public and private organizations are investing in cybersecurity as it is increasingly acknowledged that security is a factor for success and a condition for a company or brand to be trusted. Worldwide security spending will reach $174.7 billion in 2024.

INCREASED SPENDING IN CERTAIN SECTORS

Cybersecurity spending will be particularly visible in the healthcare, banking & financial, insurance, technology, telecommunications, media, public and social sectors. Nevertheless, considering upcoming legislation and future regulatory obligations such as in the EU, it is expected that other sectors will also allocate a bigger part of their budget to cybersecurity.

NEW TECHNOLOGICAL TOOLS FOR CYBERSECURITY – NOTABLY AI AND MACHINE AUTOMATION

The tools deployed in order to tackle cyber threats become increasingly sophisticated. It has been forecasted that passwordless authentication and security and control applications within cloud environments, such as CASB (Cloud Access Security Broker) and CWPP (Cloud Workload Protection Platforms), will be among the most influential cybersecurity technologies in the future. AI will also become a central technology, as well as machine learning, which will allow devices to autonomously self-diagnose and self-secure. AI may also evaluate users' behavior and detect indicators of cyber-attacks through the correlations of events.

INCREASED CAPACITY BUILDING

Cybersecurity training is set to play an increasingly relevant role within organizations, as well as the simulation of security incidents and attacks, with stakeholders cooperating across the value-chain to tackle cyber challenges.

GROWTH OF PRIVATE-PUBLIC PARTNERSHIPS TO DEAL WITH CYBER THREATS

Public-private cooperation is foreseen to play an increasingly significant role in tackling cyber challenges, including through the exchange of data and expertise, in the definition of public policies, in capacity-building actions, as well as in cybersecurity certifications and standards.

GROWTH OF THE SECURITY INDUSTRY

The global cybersecurity market is expected to grow from 167.1 billion dollars in 2019 to 248.26 billion dollars by 2023.
Security services will be the largest and fastest-growing segment of the security market, followed by software.

INCREASED REGULATORY REQUIREMENTS AND SANCTIONS ARISING FROM CYBER INCIDENTS

New cybersecurity rules are set to be approved in the EU, such as the Proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS II) and a Directive on critical entities' resilience (CER). In the financial sector, the proposed Digital Operational Resilience Act (DORA) is also set to bring new more demanding obligations. In Portugal, Decree-Law 65/2021 was approved, which establishes the legal framework applicable to cyberspace security and defines cybersecurity certification obligations.
In addition, many sectors have their own specific security provisions, with the GDPR specifically addressing data breaches. The complexity of the legal rules with impact on cybersecurity is increasing, as are fines, requiring increased attention by all stakeholders.

Organizations must proactively develop and implement a **cybersecurity strategy** under the principles of prevention, reaction and monitorization. The implementation of such a strategy necessarily entails a holistic approach and analysis so as to identify and better address the legal, operational, economic and reputational risks.

WHAT ACTIONS FOR 2022

CYBERSECURITY ASSESSMENT

Map your organization's processes and documentation and assess its level of cyber resilience, including with relation to suppliers, partners, employees and clients.

CYBERSECURITY RESILIENCE

Devise internal cybersecurity policies, install technical and organizational measures, comply with required certifications and applicable standards, carry out audits and take out insurance.

CYBERSECURITY INCIDENT RESPONSE

Identify and register the cyber incident, collect evidence, perform risk analysis, perform containment and recovery actions, send all required communications and notifications to relevant parties and regulatory authorities, and devise and implement a mitigation strategy in accordance with the identified risks.

AWARENESS AND CAPACITY-BUILDING

Perform employee training regularly and implement internal programs increasing cybersecurity alertness. Set up capacity-building cooperation programs with your business partners and service providers.

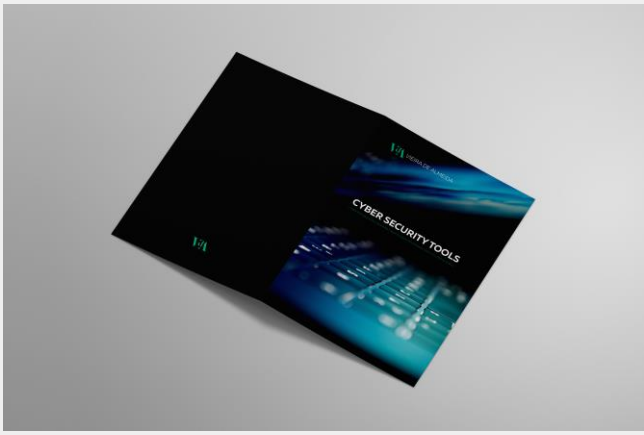
CONTINUOUS MONITORING

Cybersecurity is an ongoing process. You should ensure that your cybersecurity strategy complies with dynamic regulatory and market updates.

VdA CYBERSECURITY TOOLS

VdA developed a set of **Cybersecurity Tools** to help organizations tackle cybersecurity's increasing legal and regulatory complexities.

Comprising three programmes (Cyber Resilience Programme, Cyber Incident Response Programme and Cyber Focused Business Programme), VdA Cybersecurity Tools will ensure that your organisation is fully prepared to respond to cybersecurity challenges through a holistic approach that takes into consideration the particularities of your organisation and your sector.



www.vda.pt

MAGDA COCCO
Head of Practice Partner
mpc@vda.pt

INÊS ANTAS DE BARROS
Partner
iab@vda.pt

MARIA DE LURDES GONÇALVES
Managing Associate
mlg@vda.pt

HELENA CORREIA MENDONÇA
Principal Consultant
hcm@vda.pt