VIEWPOINT

ARTHUR D LITTLE
2024

BIG DATA? BIG SECURITY!

How to protect your data from the increasing risk of cyber threats

The revolution introduced by the digitization process has made it possible to generate and collect increasingly expanding volumes of data. As a result, public and private organizations must define new strategies, design and implement protection systems, adapt their operational models, and learn to manage information by mitigating the risks linked to cyber threats — while remaining in compliance with the provisions of the main regulations in force. In this Viewpoint, we describe the measures organizations must take to mitigate risks.

AUTHORS

Mario Nico

Michael Kolk

Dario Garante

Riccardo Calogiuri

Lorenzo Cimarelli

MORE DATA, MORE ATTACKS!

Data is a fundamental business asset. Its loss or compromise can significantly harm companies and organizations in terms of financial performance, brand reputation, or loss of customers. Whether an organization leverages data to run its business, or data is a byproduct of conducting day-to-day operations, or the institution sells data assets as a one-off product, all data must be managed, protected, tracked, and updated. The economic value of data is further amplified as enterprises go through digital transformation, leading to increased data production.

Organizations have not yet grasped all aspects concerning data, including these important considerations:

- **Who** can access the data, and **what data** can they see?
- How can data be protected from illicit **access attempts**?
- How **competent** are **users**, and how do you ensure they continue to be informed about **risks** associated with processing of information?

In the Viewpoint "The Cyber Battlefield," Arthur D. Little (ADL) shared several strategies for companies to establish cybersecurity capabilities. While most data security breaches (74%, according to Verizon) are generated by internal user error, employing IT systems such as privileged access management allows organizations to govern user access to information, limiting the risk of unauthorized access. At the same time, it is possible to adopt solutions (e.g., security information and event management) to control who accesses what and monitor how data is changed. Such IT systems enable organizations to detect abnormal behaviors that can be traced back to malicious access attempts, allowing timely intervention. Investments like these enable organizations to respond proactively to the risks generated by cyberattacks.

CYBERATTACKS HAVE INTENSIFIED SINCE END OF THE FIRST QUARTER OF 2023

Nevertheless, as data increases exponentially, there has been a continuous growth of cyberattacks (although a direct correlation has not been proven). *Infosecurity Magazine* reports that cyberattacks against government agencies and public sector services increased by an astounding 40% in the second quarter of 2023 over the first quarter. BlackBerry Cybersecurity claims it stopped 1.5 million attacks over the 90 days from March to May 2023, of which 55,000 targeted the public sector. Analysis of data shows that cyberattacks have intensified since end of the first quarter of 2023. According to BlackBerry, the highest distribution of cyberattacks during that period included:

- Financial institutions
- Healthcare services and equipment
- Government/public entities
- Critical infrastructure

Further analysis of the types of attack reveals the reasons behind a cyberattack fall into two categories:

1. **Economic.** Perpetrated by criminal organizations, these attacks take advantage of a variety of available tools (e.g., ransomware, distributed denial-of-service [DDoS], malware, phishing) to return a profit. As an example, consider the case of the UK's Royal Mail, which, following a ransomware attack in January 2023, refused to pay the £67 million (about US $85 million) the perpetrators demanded.

2. **Political.** These attacks are, at their base, related to political issues (sometimes local but more often international). They can often be traced to acts of activism but may also be used to foment cyber wars and can be compared to acts of terrorism. For example, in November 2023, Russian hackers breached 22 Danish power companies in the context of tensions between the Russian Federation and the NATO blockade.

Considering the high costs of data breaches in terms of money (IBM estimates the average cost of a data breach in 2023 to be US $4.45 million), time, and reputation, the importance of preventing attacks is abundantly clear. For this reason, organizations must:

- **Understand the regulatory landscape** — to unlock the value of data; protect data from unauthorized access, disclosure, alteration, or destruction; and maintain the privacy of individuals and organizations
- **Commit to increasing investments in defensive technological solutions** — with the goal of better understanding competition, customers, and technological trends; supporting business growth; and ensuring secure management of information
- **Adopt standards and frameworks and define business practices** — to guarantee a qualitative and quantitative level of information security, continuously adapting to the growing number of attacks and balancing data sharing with protection (see the ADL Viewpoint "Harnessing External Data Sharing to Unlock Transformative Collaboration").

REGULATORY LANDSCAPE TRANSFORMATION

According to DemandSage, an average of 328.77 million terabytes of data is created every day. But the ability to ensure the proper management and protection of data remains elusive. While from a security and privacy perspective the EU General Data Protection Regulations (GDPR) has raised a shield to defend information, the regulation of big data use still awaits final approval of the EU Data Act, which is joined by the AI Act (legislation focused on regulating data analysis processes based on artificial intelligence [AI] technology). Both legislative acts face a path of about 12 months (end of 2024) awaiting definitive approval by the EU. Thereafter will begin the process in which the acts are transposed into national law by EU countries.

Although GDPR's reach extends only to personal data, the Data Act encompasses both personal and nonpersonal data, making its range of application notably wider. The Data Act aims to eliminate data-access hurdles for both public and private organizations, making it simpler to transfer data among service providers and encouraging a broader range of participants, including small and medium-sized enterprises, to engage in the data economy. These new regulations will empower consumers and businesses to have a voice in determining the usage of data produced by their connected devices.

Additionally, with increasing integration of AI systems into everyday life, issues surrounding data protection and ethical considerations have come to the forefront. Cybercriminals could use AI to easily develop malware that can discover previously unknown vulnerabilities or evade detection and create sophisticated phishing attacks. GDPR supports the creation of AI and big data applications that effectively strike a balance between data protection and other societal and economic interests yet offers limited guidance on accomplishing this objective. Consequently, the AI Act aims to regulate AI through a risk-based approach, which differentiates compliance obligations based on the potential risk that intelligent software and applications may pose to fundamental rights. The higher the risk, the more substantial the compliance requirements and responsibilities for the creators of smart applications.

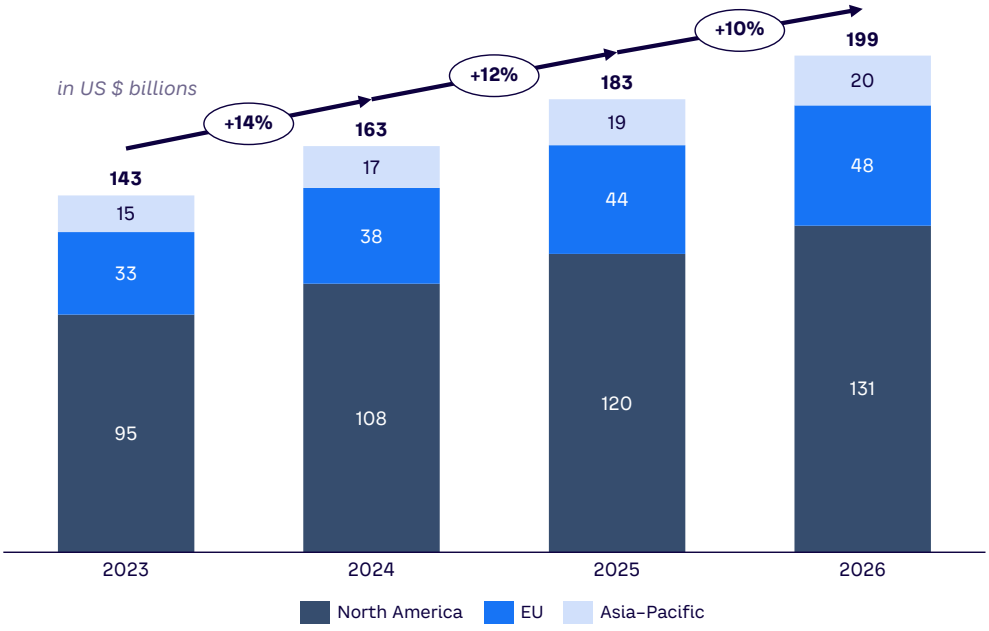
The completion of the regulatory path for both the Data and AI Acts by EU countries will require public and private organizations to adapt within certain time frames and change processes, committing new budgets and adapting business models to ensure compliance.

COMMITMENT TO INVESTMENTS

The growth in data availability is leading companies, both public and private, to make ever greater investments in the acquisition of tools and technologies for their management. The aim is to know about the competition, customers, and innovative technological trends and tools; to support business growth through the planning and implementation of effective strategies; and to ensure the secure management of information.

But while investments have focused on the acquisition of know-how for the analysis, processing, and visualization of information and technological tools like business intelligence, data analytics, and AI systems, a report published by the European Union Agency for Cybersecurity (ENISA) highlights numbers linked to the main growth drivers of information security spending in 2023. The report identifies the main drivers of the increase as **hybrid working,** transition from virtual private networks (VPNs) to zero-trust network access, and the move to **cloud-based deployment models.** The study estimates an overall growth in spending in 2023 of $143 billion, and the estimate for 2024 stands at $163 billion, with a growth of up to 14% (see Figure 1).

Figure 1. Information security spending per region, 2023–2026



Source: Arthur D. Little, ENISA

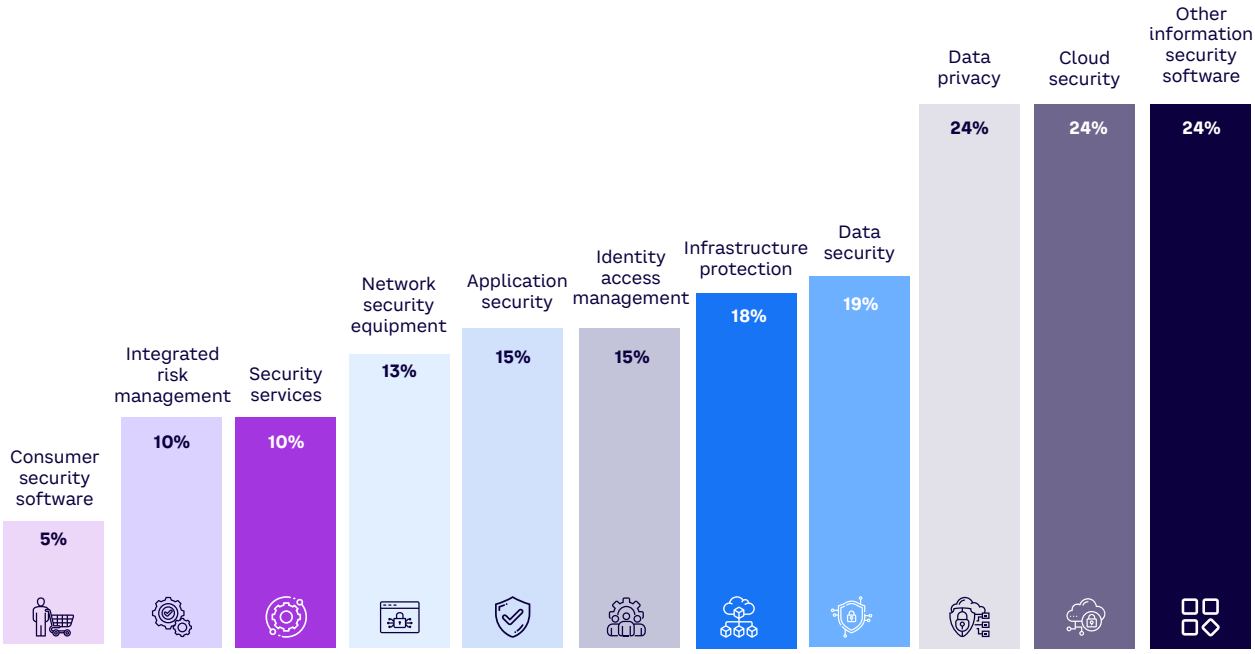
GROWTH IN DATA AVAILABILITY IS LEADING COMPANIES TO MAKE EVER GREATER INVESTMENTS IN THE ACQUISITION OF TOOLS AND TECHNOLOGIES FOR THEIR MANAGEMENT

The report predicts sustainable growth through 2026, with double-digit percentages every year. By geographical area, North America represents, on average, two-thirds of annual global spending. The gap between North America and other areas highlights a greater focus on security issues in this region and emphasizes the need for other areas to increase investments to bridge the technological and cultural gap.

According to the ENISA report, the largest increases in spending in 2024 concern **cloud security** (+24% year-over-year [YoY]), in accordance with the substantial and general migration process from proprietary on-premises architectures to cloud solutions, and **data privacy** (+24% YoY), as the organizational focus remains the processing of data for privacy purposes (see Figure 2).

The factors behind these numbers are linked to the growing risk of cyber threats as well as the changes affecting organizations and their operating models in the process of adapting to the new business paradigm, which acknowledges data as a fundamental asset for companies, both public and private. This value makes the level of security implemented and perceived increasingly critical: first, to guarantee regulatory compliance and secure the value that the company will be able to generate from access to information, and second, as an element that is of concern to stakeholders and shareholders.

Figure 2. Growth in worldwide end-user spending in security and risk, 2023–2024



Source: Arthur D. Little, ENISA

APPLYING PROPER FRAMEWORKS & BUSINESS PRACTICES

A structured framework is crucial for effective information security management. In considering information security and personally identifiable information (PII) protection, organizations can refer to widely recognized standards such as ISO/IEC 27001:2022 or the NIST Cybersecurity Framework (CSF). These standards offer structured frameworks and best practices for evaluating and mitigating information security risks. The adoption of an organizational framework can enhance time to market by standardizing processes, automating security and privacy compliance, and establishing consistent measures.

Table 1 highlights the main characteristics of the two frameworks, but it is important to specify that these frameworks often cover the same areas, such as identifying risks, implementing controls to reduce risks, and monitoring performance. An organization can integrate the frameworks synergistically to create a holistic approach to cybersecurity.

Adopting a standard framework allows organizations to achieve a series of benefits, including:

- **Information security awareness** — enabling the implementation of robust measures for safeguarding sensitive information
- **Risk mitigation** — gaining a deeper understanding of risk management and providing the ability to identify vulnerabilities, assess risks, and implement strategies to mitigate them
- **Regulatory compliance** — complying with relevant laws and evolving regulations, providing a proactive approach to maintaining information security
- **Enhanced reputation** — increasing an organization's reputation and providing greater confidence of an organization's customers and partners, fostering better relationships and creating additional business opportunities
- **Cost savings** — following the initial investment, prompting medium/long-term benefits due to increasing information security "culture," decreased likelihood of breaches, and subsequent reduction in legal fees and reputational damage

Table 1. Approaches of different frameworks

	ISO/IEC 27001:2022	NIST CYBERSECURITY FRAMEWORK 2.0
Focus	Improving an organization's **information security management system**	Managing & reducing **cybersecurity risks** to networks/data
Brief description	Provides systematic approach to managing sensitive company information, including data management, access controls & risk management	Provides a framework that any organization can use to elevate the maturity of its cybersecurity risk programs
Number of requirements	**93 controls** divided between **4 themes**: 1. People (8 controls) 2. Organizational (37 controls) 3. Technological (34 controls) 4. Physical (14 controls)	**6 functions** to customize cybersecurity controls: 1. Identify 2. Protect 3. Detect 4. Respond 5. Recover 6. Govern
Expected cost	Involves series of **audits & certifications** that involve greater expense	**Voluntary**, allows organizations to implement the standard using preferred pace & resources

Source: Arthur D. Little, OneTrust

In general, the ISO/IEC 27001:2022 standard is useful for operationally mature organizations that aim to put in place or improve their entire information security management cycle and are seeking certification to demonstrate the company's dedication to security and compliance. Conversely, the NIST CSF is more suited to evaluating maturity in the first stages of developing a cybersecurity risk management plan or in attempts to mitigate prior failures or data breaches.

By aligning with these well-established standards, organizations can methodically identify and address potential threats, safeguarding both information security and privacy, while demonstrating their commitment to compliance and data protection. It is important to remember that there is no one-size-fits-all approach, so every organization must choose the model that best suits its needs.

Case study: Protecting water resources in Italy

A project in Italy sought to enhance the information assets of the surveillance system for territory governance and the protection of water resources. Its primary objective was to defend water sources from anthropogenic and natural threats through an integrated monitoring network to assess the status of water resources and soil.

ADL designed a system to monitor the quality, availability, and safety of water by allowing authorities — on the basis of their responsibilities and competences — to take the measures necessary for mitigating criticalities and risks, promoting appropriate prevention actions.
The project's complexity centered around the management of a critical amount of vital data. In addition, the information management system needed to ensure that the data could support various authorities' investigations, particularly in the detection of environmental crimes and in allowing for those investigations to be carried out to ensure their nonrepudiation.

The system, structured to support the customer's functions of planning, management, and monitoring of existing resources, as well as communication to and from the outside, was built utilizing data and information from:

- Internet of Things (IoT) sensors
- Remote sensing through optical and radar images acquired by the Sentinel-1 (radar) and Sentinel-2 (optical) constellations of the European Space Agency (ESA) Copernicus program
- Video surveillance
- Web application for viewing geospatial data and monitoring dashboards

The system included a segregated network, protected by a multifactor authentication firewall, externally accessible only via VPNs and with firewalls installed on individual servers. The architecture was designed to manage information in compliance with ISO/IEC 27001:2022 standards to ensure maximum security of strategic information, while internal processes were formulated to define the correct collection and maintenance of information in compliance with GDPR. To this purpose, ADL supported the implementation of privacy fulfillment using privacy by design, risk analysis, and data protection impact assessment.

CONCLUSION

SECURITY CONTINUOUS IMPROVEMENT

ORGANIZATIONS MUST MANAGE THE EVOLUTION OF REGULATIONS AND TECHNOLOGY TRANSFORMATION

Increases in data and digitalization processes have led to an escalation of cyberattacks against companies and institutions as well as to a continuously evolving regulatory environment and a need for companies to constantly adapt to the changing dynamics of the data economy. Thus, organizations must invest in technologies for prevention and protection, while at the same time provide communications and trainings to ensure their people are aware of the culture of security as good business practice. Overall, organizations must manage the evolution of regulations and technology transformation, paying particular attention to:

1. Assessing information security maturity and the level of risk exposure
2. Identifying and adopting frameworks to adapt to international standards and regulatory compliance requirements
3. Defining an adequate budget and embracing technology improvements to proactively respond to the risks of cyberattacks

NOTES

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.