## Axis 6: Cybersecurity

In the digital age, cybersecurity has transcended its past role as a mere safeguard to become a fundamental pillar of operational integrity and trust. As organizations increasingly digitalize their operations, the importance of robust cybersecurity measures has never been more critical. Accordingly, this sixth axis of digital transformation explores how deeply an organization has ingrained security practices into its digital and operational fabric. The relentless evolution of cyber threats means that a proactive stance on cybersecurity is not just advisable; it is imperative for protecting sensitive customer data, ensuring privacy and maintaining the trust that is so crucial to sustaining reputation and financial viability.

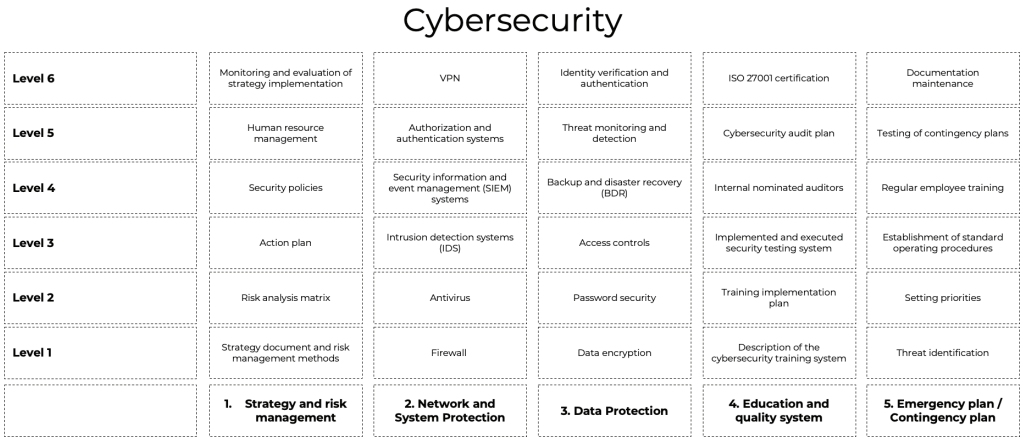


Figure 16

This axis evaluates an organization`s cybersecurity maturity across five distinct but interconnected areas: strategy and risk management, protection of networks and systems, data security, education and training, and emergency planning. Each area is assessed on a graduated scale that corresponds to the depth and sophistication of cybersecurity measures in place. From the basics of securing network perimeters to the complexities of managing a comprehensive emergency response, this axis provides a structured framework to gauge how prepared an organization is to defend against and respond to cyber incidents with the potential to disrupt operations and compromise data

integrity. As we elaborate on the specifics of each area, we underscore the critical need for an integrated approach to cybersecurity, one that stays in step with both technological advancements and emerging threats. The level of an organization`s digital development in the area of cybersecurity is assessed in five areas: strategy and risk management, network and system protection, data protection, education and quality systems, and emergency plans. Each area is evaluated on a scale from level one to level six.

## Area 6A. Strategy and risk management

Strategy and risk management emphasizes the foundational need for a coherent and comprehensive approach to security within an organization. This entails the establishment and enforcement of a robust cybersecurity strategy and policy that outlines the organization`s security objectives, principles, standards and procedures. They also delineate the roles and responsibilities associated with managing and mitigating risks. This strategic framework is crucial for identifying potential cybersecurity risks. Through systematic analysis and assessment, the organization can prioritize these risks and apply the most effective risk management techniques to minimize exposure and enhance its defence against potential security breaches. This strategic preparation is vital for building a resilient infrastructure that can withstand and rapidly recover from disruptions caused by cyber threats.

**Level 1. No cybersecurity strategy or policy.** The organization has not developed or implemented a cybersecurity strategy or policy. There are no defined goals, standards or security procedures. Risk management is impossible, and the organization is exposed to serious threats.

**Level 2. Risk analysis.** The strategy involves a cybersecurity risk analysis that determines threats and risks associated with the organization`s activities, the assets exposed to risk (such as customer data) and the development of preventive measures. For example, in a financial institution, risk analysis may include assessing threats to payment systems, identifying vulnerable assets such as customer data, and developing preventive measures.

**Level 3. Action plan.** The strategy includes, in addition to risk analysis, an action plan that specifies the precise steps the organization will take to minimize risk. In a bank, the action plan may include regular software updates, security training and the implementation of incident response procedures.

**Level 4. Security policies.** The strategy also describes cybersecurity policies that define the standards and procedures the organization will use to protect its assets and data. In a company, security policies may include rules for setting strong passwords, data and system access procedures, and guidelines for software updates.

**Level 5. Strategy includes human resource management.** This may cover training the organization`s staff in the skills and knowledge needed to effectively counter cybersecurity threats. For example, the company includes regular security training for employees and specialized courses for the IT team, increasing readiness to respond to cybersecurity threats.

**Level 6. Monitoring and assessment.** The strategy includes plans for monitoring and assessing the effectiveness of cybersecurity actions to ensure that the strategy is working and being updated as the organization`s needs change. Examples of solutions include regular audits, penetration tests and log analysis to monitor and adjust the cybersecurity strategy to current needs.

## Area 6B. Protection of networks and systems

The protection of networks and systems focuses on the deployment of robust technologies and methodologies essential for safeguarding an organization`s digital infrastructure. This includes the installation of firewalls, intrusion detection systems and antivirus software, which serve as the first line of defence against cyber threats. Additionally, implementing access control systems ensures that sensitive information and critical systems are accessible only to authorized personnel. Data encryption and routine backups further fortify security by protecting data integrity and ensuring that, even in the event of a breach or data loss, the organization can recover swiftly and effectively. These protective measures are integral to maintaining the security and operational continuity of the network and system infrastructure.

**Level 1. Firewalls.** This type of software or device acts as a barrier controlling traffic between different segments of the network, allowing only trusted sources to access sensitive financial data. This ensures effective protection against potential threats. For example, for companies in the financial industry, such as banks or investment firms, a firewall is a key tool for protecting against unauthorized access to networks.

**Level 2. Antivirus.** Companies install antivirus programs on all their computers to regularly scan files and systems, detecting and removing malicious software. This is crucial for, for example, maintaining the security of medical information and system stability. In the healthcare sector, where patient data confidentiality is a priority, antivirus programs serve as the first line of defence against malicious software.

**Level 3. Intrusion Detection Systems.** In case of suspicious activities, such as intrusion attempts or attacks on control systems, these systems immediately generate alarms, allowing for a quick response and risk minimization. For example, in the energy sector, threat detection systems are essential for monitoring network traffic and securing energy infrastructure.

**Level 4. SIEM or IDS.** Upon detecting abnormalities in delivery or attempts to compromise data, Security Information and Event Management systems and Intrusion Detection Systems analyse data from multiple sources and

generate alerts or reports, enabling an effective response and ensuring operational continuity. These systems are used in the transportation sector, for example. Here, where complex logistics networks and data management are commonplace, incident detection systems are essential.

**Level 5. Authorization and Authentication Systems.** These systems verify the user`s identity and access level. In the education sector, for example, where there is a need to secure access to university resources, authorization and authentication systems are indispensable. Students and staff must provide unique identification data and passwords to access educational materials.

**Level 6. VPN.** Virtual Private Networks are used as a fundamental part of cybersecurity in, for example, the e-commerce industry, where secure transmission of financial data is a priority. Online merchants use VPNs to ensure a secure connection between different geographical locations, protecting sensitive data from interception. This allows for the secure transmission of financial information over public networks while protecting customers.

## Area 6C. Data security

This area evaluates the stringent measures an organization employs to protect sensitive data from unauthorized access and breaches. It emphasizes strictly limiting data access to authorized personnel based on predefined roles and permissions, thereby mitigating the risks associated with internal threats or inadvertent data exposures. Furthermore, this area assesses the methods used to safeguard data during transmission and storage, which include robust encryption techniques and rigorous authorization protocols. Adherence to data minimization principles – collecting and processing only the data absolutely necessary for specific purposes – further enhances the security posture, ensuring compliance with regulatory standards and reducing the likelihood of data vulnerabilities.

**Level 1. Data encryption.** This involves using cryptographic algorithms to secure data from unauthorized access and reading. This requires that encryption algorithms be implemented, monitored and updated and that employees be trained in the correct use of encryption tools.

**Level 2. Password security.** This involves enforcing the use, regular changing and secure storage of strong passwords. This requires implementing a password security and storage management policy – for example, in encrypted form.

**Level 3. Access controls.** Access to data is limited to authorized users only based on roles and permission levels. This involves defining roles and permission levels for users, implementing access monitoring and audit systems and training employees in adhering to principles of access control.

**Level 4. BDR.** Backup and Disaster Recovery involves regularly creating backup copies of data so that, in the event of the loss of original data, they can be effectively restored. This requires that a backup strategy be established, that the process of data restoration from backup copies be tested, and that the backup strategy be regularly adjusted to changing needs.

**Level 5. Monitoring and threat detection.** Tools are used that monitor networks and systems to detect abnormalities and threats. This involves

implementing solutions that monitor systems and network traffic, training monitoring personnel to respond to security alarms and continually updating monitoring tools.

**Level 6. Identity verification and authentication.** Preventing unauthorized access to data and systems by unauthorized individuals requires the implementation of identity verification systems, such as biometric scanners or digital certificates, and, of course, training.

## Area 6D. Education and training

This area highlights the importance of continuous learning to enhance employee awareness and capabilities in countering cybersecurity threats. Training starts with fundamental cybersecurity hygiene – creating strong passwords, identifying suspicious links and reporting anomalies – and progresses to cover more sophisticated threats like advanced phishing, social engineering and ransomware. Regular simulations and knowledge tests assess training effectiveness and identify areas needing improvement, thereby ensuring that training evolves to keep pace with cybercriminal tactics. This ongoing education is critical, making employees proactive defenders and an essential part of an organization`s cybersecurity strategy, to build a resilient, aware workforce capable of minimizing security incidents.

**Level 1. Description of a cybersecurity training system.** This system is used to plan, organize and conduct cybersecurity training in the organization. The description sets precise training goals, schedules and topics to be covered, and it identifies appropriate trainers. In large enterprises, such a system helps identify training needs.

**Level 2. Implementation plan for cybersecurity training.** This plan is crucial for increasing employee awareness of threats and ways to minimize them. It includes various forms of training, from traditional face-to-face sessions to online courses and attack simulations. It is also important to determine indicators for monitoring training progress and to adjust the plan accordingly.

**Level 3. Security testing system.** This tool identifies weaknesses in the IT system, allowing them to be fixed before attackers can exploit them. Implementation and regular security testing help minimize the risk of cyberattacks.

**Level 4. Internal auditors.** Employees are trained as internal auditors who conduct regular internal audits of cybersecurity. Their goal is to assess the effectiveness of systems and procedures, contributing to continuous improvement in this area.

**Level 5. Cybersecurity audit plan.** This schedules and determines the scope of internal and external audits to assess effectiveness and compliance with the organization`s cybersecurity policies and procedures. It also ensures compliance with applicable standards and regulations on information security.

**Level 6. ISO 27001.** This international standard for information security management is used to certify organizations that have implemented a sufficient information security management system. Certification attests to high-quality risk management and protection of confidential information in the organization. This certificate builds trust with customers and business partners and contributes to the company`s development.

## Area 6E. Emergency planning

Emergency planning in cybersecurity involves developing detailed strategies for swift and effective response to cyber incidents. This comprehensive approach includes regular risk assessments, audits and the identification of critical areas to establish clear action priorities during emergencies. Effective emergency plans ensure rapid response capabilities that minimize operational disruptions and losses by quickly restoring critical system functions. Moreover, this plan encompasses ongoing employee training, regular testing of response procedures and meticulous maintenance of documentation to ensure readiness and compliance with standards. As an integral part of a cybersecurity strategy, emergency planning not only helps in effectively managing incidents but also reinforces organizational trust by demonstrating to its stakeholders and customers the company`s degree of preparedness, thereby safeguarding business continuity and reducing risk exposure.

**Level 1. Threat identification.** The first step in developing emergency plans is to identify potential threats to the organization`s information systems and data. A security audit and risk analysis are conducted to determine areas requiring special protection.

**Level 2. Defining priorities.** The next stage is determining priorities in the event of an incident. The emergency plan must precisely define which parts of the system require immediate repair and restoration.

**Level 3. Defining procedures.** The emergency plan should contain detailed procedures for handling incidents. These procedures describe specific steps to be taken to limit the effects of an attack or a failure of information systems.

**Level 4. Regular employee training.** Another element of developing emergency plans is regular employee training in emergencies. These training sessions cover both technical aspects and security procedures.

**Level 5. Testing emergency plans.** After defining emergency plans, it is important to regularly test them in practice. These tests should include various incident scenarios and be conducted in a controlled manner. Regular

testing allows adjustments to be made to emergency plans based on changing conditions and threats.

**Level 6. Documentation.** To ensure the effectiveness of emergency plans, it is necessary to keep accurate documentation. This documentation includes information about procedures, test results and implemented changes. This allows for the rapid identification of weaknesses and introduction of corrections. Precise documentation is important if incidents are to be responded to swiftly and their harms minimized.

In conclusion, cybersecurity is often underappreciated until a crisis unfolds. Much like safety measures in traditional industries, where the value of a Safety Officer is often only recognized following a serious incident, the critical importance of robust cybersecurity measures tends to be realized in hindsight. As enterprises expand their digital footprints, the necessity for both technical and non-technical measures to safeguard information, systems, and software becomes increasingly imperative. This aspect of digital transformation is not merely a precaution; it is an essential component of maintaining trust and operational integrity in the digital age. Neglecting this could lead to severe consequences, making it essential for businesses to prioritize and continuously enhance their cybersecurity strategies.

# Index

6V
Adobe
AI, Artificial Intelligence
Alibaba
AlphaGo
Altman, Sam
Amazon
API, Application Programming Interface
AR/VR, Augmented Reality/ Virtual Reality
B2B, business to business
Ballmer Steve
Bennis, Warren
Bezos, Jeff
Big Data
Black swan
Blik
Boeing
Bolt
Booking.com
Branson, Richard
Buffett, Warren
butterfly effect
C&D, Connect and Develop
ChatGPT
Christensen, Clayton
Cisco
CMMS, Computerized Maintenance Management Systems
Cooperators
CRM, Customer Relationship Management
customer experience
DBR77
Deep Blue
Deep Mind
Devol, Georg
Digital 2022 Global Overview Report
Digital Change Management
Digital Roadmap
Dropbox
EDI, Electronic Data Interchange
Eight-step model (see: Kotter`s eight-step model)
ERP, Enterprise Resource Planning
ETL, Extract, Transform, Load
Farley, Jim
FMEA, Failure Mode and Effects Analysis
Ford (Motor Company)
Ford, Henry
Frog (see *Żabka*)
GAI, General Artificial