WRITTEN BY

**BIBIÁNA ŽIGOVÁ**
Information security Senior manager
TPA Slovakia

# INFORMATION SECURITY STRATEGY

In today's digital landscape, safeguarding economic and business information is crucial for success. With data playing a pivotal role across different sectors, ensuring data security is paramount to prevent losses, corruption and legal repercussions while also safeguarding the company's credibility and reputation. While the state of information and cybersecurity varies globally, certain universal trends and challenges persist.

### THE CURRENT LANDSCAPE

Cyber threats are escalating and can come in various forms, such as ransomware, phishing and infrastructure attacks, and target organizations, government bodies and individuals alike. Attacks on critical infrastructure like power grids and healthcare systems pose significant risks to society and the economy. This escalating threat is prompting governments to introduce stricter cybersecurity regulations, placing cybercrime on the same level as physical crime.

### RISK ANALYSIS

Risk analysis involves identifying, evaluating and managing organizational risks while aiding informed decision making to mitigate potential threats. This process involves risk identification, assessment and management, fostering better governance, decision making and regulatory compliance while enhancing efficiency and preventing adverse events.

### IDENTIFYING RELEVANT INFORMATION

Prioritizing critical data such as trade secrets and financial records is the first step in information protection, by focusing security efforts on vital areas. You should create a catalogue of priority information, documents and assets. Then assign a degree of Confidentiality, Integrity and Availability to each item using the simple, easy-to-remember CIA rule.

### IMPLEMENTING SECURITY PROTOCOLS

Deploying robust security protocols including firewalls, encryption and access controls is imperative. Regular updates and testing ensure efficacy, especially in encryption, rendering data unreadable to unauthorized access. Make sure you consult cybersecurity experts to ensure proper hardware and software configuration. Be sure to employ disk encryption and data leak protection to avoid data leaks from inside the organization.

### EMPLOYEE TRAINING

Educating employees about cybersecurity risks and fostering a security-conscious culture are crucial in mitigating vulnerabilities. We suggest you prepare a simple but effective training course on phishing and internet threats for your employees and include a cyber game with prizes in your teambuilding activities. Policies and Procedures Establishing clear policies and procedures regarding data protection and access ensures consistency and compliance while enhancing organizational security. This framework is key to achieving goals, maintaining quality and improving employee performance. Draw up guidelines on your password policy, access policy, rules for working with IT devices for both employees and administrators, and security zone policy within the office. Make sure you update these guidelines regularly and familiarize employees and external collaborators with their wording.

### MONITORING AND THREAT DETECTION

Utilizing threat monitoring systems aids in identifying and resolving security incidents promptly. Be sure to implement infrastructure monitoring, collect logs, implement special software for monitoring activities on the network, on endpoints, etc. The more relevant notifications you have from your infrastructure, the faster you will discover potential risks and be able to mitigate them.

### FIREWALL AND ANTIVIRUS SOFTWARE

Install and regularly update firewall and antivirus software. These tools help protect systems from malware and cyberattacks. Prevent your users from uninstalling antivirus software on their workstations and installing any free software. Use VPN access policy for information systems and applications.

### ACCESS MANAGEMENT

Limit access to sensitive information to only those who really need this data for their work. Access control is an effective way to minimize the risk of unauthorized access. Ensuring only authorized persons have access to confidential information can be achieved by using various security measures, such as passwords, biometric identification and physical access restrictions. Implement data leak protection tools. These will allow you to manage access while preventing unwanted data leaks. Use a very simple triangle for access management:

- Something you know (password, PIN code)
- Something you have (mobile phone with multifactor authentication)
- Something you are (biometric data, face recognition, fingerprint)

### BACKUP

Creating regular data backups and developing a recovery plan is essential to minimize damage in the event of a crash or cyberattack. Ensuring data is backed up regularly and can be restored quickly can be critical to a business's survival in the event of a crisis. Don't forget to test your backups regularly. Backups should follow best practice using the 3-2-1 equation. This means:

- 3 copies of data
- on 2 types of media
- with 1 type of media to be stored outside of the room where the other media are kept

### CONTINUITY MANAGEMENT

Have a security incident response plan, i.e. a continuity plan, in place so that you can act quickly in the event of an information leak or cyberattack. Don't forget to update and test your continuity plans regularly. In the event of an incident, you must remember that there will be panic. Therefore, it is essential to have a plan detailing the steps to be taken to minimize any negative impact. Be sure to have a printed version of this plan available as well, because you might not be able to access your plan digitally in the event of an infrastructure failure. At the same time, training and testing can also help raise awareness about cyber security.

### CONCLUSION

Comprehensive information security measures bolster resilience against cyber threats and minimize data loss risks. Protection of economic and business information is an ongoing endeavor that is vital for sustained competitiveness in the market. Implementing these strategies instills confidence in information security, ensuring organizational longevity and success.