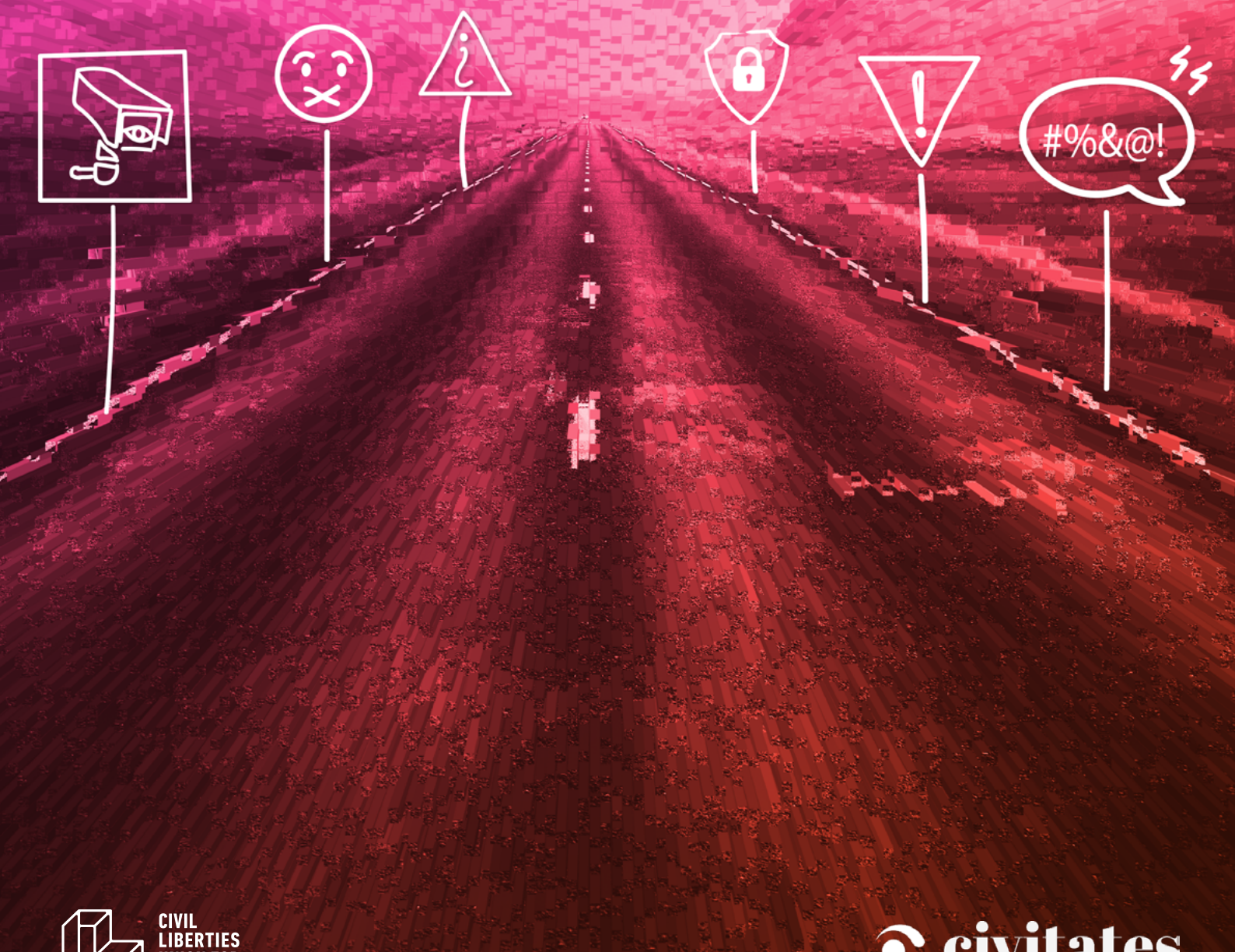
# CYBER SECURITY GUIDE FOR PROTECTING ONLINE CIVIC SPACE

## Seven questions to help improve the digital self-defence capabilities of your organisation

November 2023




CIVIL LIBERTIES UNION FOR EUROPE

civitates

# Table of contents

# Executive summary

There is almost no organisation without obligations to protect some form of sensitive or confidential data in their possession. Whether personal data of newsletter subscribers, payment details for donations processed, preferences of beneficiaries supported, event registrations, future plans, all need protection.

Organisations need to find a way to implement security measures specific to their specific needs and challenges. Security needs context, a clear scope and objectives. And like safety, security is rarely absolute. It is possible to have accidents even in safe environments; and it is also possible to endure dangerous environments or situations without harm or damage. However, staying safe and secure does not only come down to luck: perspective, preparation, and prioritisation also matter. In the field of information security, this translates to awareness of cyber risks.

As much as technology plays an important role in shaping security challenges, at the core of it, security is not an IT problem. Maintaining a good security posture will depend on each member of an organisation, and their ways of working. Getting the basics right, understanding risk-based decision making, knowing what needs protecting: this guide offers considerations for aligning the three key components – people, process, and technology.

This publication suggests approaches and highlights important considerations for organisations of all shapes and sizes to find the answers to seven questions that are essential for assessing and improving their overall security readiness:

1. What channels and techniques are used to disrupt NGOs?
   - *Understanding cyber risks*

2. What are the common impacts of disruption and compromise in the digital space?
   – *The effects of a data breach*

3. What needs protecting?
   – *Knowing value*

4. Who does the organisation need protecting from?
   – *Learning about malicious actors*

5. What are the essential security measures for cyber hygiene and digital self-defence?
   – *Protecting the organisation*

6. How to work towards resilience?
   – *Incident response and recovery*

7. Why even the best protected organisations must stay vigilant?
   – Continuous improvement of the security posture

The ultimate objective of the guide is to create a culture where everyone feels responsible for the security of the organisation.

# Introduction

The unprecedented interconnectedness of our times enables collaboration between diverse groups and locations, and provides broad access to vast amounts of data and information. It continues to open up new opportunities all over the globe. However, on some days the view is more dystopian: the same technologies that connect people can fuel the polarisation of public discourse, and drive us apart as we get trapped in social media filter bubbles. How do we stay safe in such an environment? What practices can our organisations adapt for digital self-defence?

Technology changes affordances. It makes some things easier. It makes other things harder. Today's communication platforms offer simple tools to reach large audiences spanning across borders. Yet, the same systems and methods can make it difficult to protect the confidentiality, integrity, and availability of our messages. In other words: today's complex technology landscape makes information security and cyber risk a growing, and ever-changing threat. The report explores practical advice for reinforcing the security posture of any organisation. It also maps out connections to other, adjacent topics and concepts that can influence the overarching security stance.

## Caveats and limitations

To keep the focus of this publication on good practice for security, and easy-to-follow measures for online safety, we note that the following topics are often discussed in context of their relationship to information security; however, they will not be covered in detail:

- data protection and privacy;
- hate speech;
- censorship;
- surveillance;
- artificial intelligence (AI) and machine learning (ML).

Information security and cyber risk are deeply interconnected with data protection and privacy. Furthermore, they have an impact on hate speech, censorship, and surveillance. These concepts also fall under the broader umbrella of digital rights. While each topic has its distinct challenges, their common thread is the need to balance security and privacy in a continuously changing digital landscape.

- Data protection and privacy: security measures underpin data protection and contribute to achieving privacy-by-design principles. Online privacy often depends on robust security controls to protect personal data from unauthorised access. In the European Union, the General Data Protection Regulation (GDPR) sets the legal

framework for this topic (see also Appendix – Standards and frameworks).

- What is the Right to Privacy: Definition, Laws, Tendencies

- Hate speech: primarily relates to content and its potential social and cultural implications. Hate speech can be used as a vector for social engineering attacks (see section on cyber risks) where malicious actors prey on emotional reactions.

- Censorship: often intersects with information security in areas like content filtering, monitoring, and the enforcement of national or organisational policies. In addition, methods used to bypass censorship (like VPNs or Tor), can be considered security tools. On the flip side, censoring entities might view these same tools as cyber risks. Moreover, platforms or individuals that are perceived to be bypassing or resisting censorship could become targets for state-sponsored cyberattacks or hacking campaigns (see section on threat actors).

- Surveillance: defence against unwanted surveillance is a fundamental aspect of information security. On one hand, state-sponsored surveillance can exploit vulnerabilities in systems and software to monitor individuals, groups or entire populations. On the other hand, the tools and techniques developed for surveillance can fall into the hands of malicious actors, increasing the cyber risk for individuals and organisations.

- Artificial intelligence (AI) and machine learning (ML): AI models, like a large language model (LLM), can be targets for adversarial attacks, tools for cyberattacks, or pieces of technology that improve the capabilities of security tools. While the broader impact (and security implications) of these systems are still to be seen, it is expected that common security principles and protective measures will continue to apply, same as to any other technology.

# Understanding cyber risks

## 1. What channels and techniques are used to disrupt NGOs?

"Cyber risk" refers to the potential for harm or loss in the digital realm. A "cyber threat" is a more immediate potential for harm, and a "cyberattack" is when that harm is being actively inflicted.

Attacks may target devices, systems and applications, data, individuals and even physical locations; all leading to a disruption of day-to-day operations. Awareness of common techniques, like forms of social engineering attacks, help in recognising malicious intent and can prevent a potentially adverse scenario.

Social engineering is a broad concept covering both digital and physical tactics, usually involving some form of direct interaction, phone calls, or physical intrusion.These all exploit human behaviour and psychology rather than technological vulnerabilities.

***Common forms of social engineering include:***

- **Phishing and spear phishing**
    - Channel: emails, messages, or social media.
    - Technique: deceptive messages designed to trick individuals into revealing sensitive or confidential information, like passwords or financial details. Spear phishing is a more targeted form of phishing where the attacker has done research on the target for a more convincing deception.
- **Business email compromise (BEC)**
    - Channel: emails.
    - Technique: also considered a specific form of phishing, where attackers compromise or spoof a business email account, often of an executive or someone in a financial role (specific subtypes of BEC, also known as CEO/CFO scam), to conduct unauthorised fund transfers or gather sensitive information. The emails sent by the attackers appear legitimate and request actions such as bank transfers or invoice payments to fraudulent accounts.
- **Vishing (voice phishing)**
    - Channel: phone calls.
    - Technique: using deceptive phone calls to trick individuals into providing sensitive information or performing actions that compromise security. As with phishing, these attacks can also incorporate impersonation techniques. The attacker pretends to be

someone else - a coworker, a bank representative or a trusted vendor - to extract sensitive information, financial details, or simply to build trust for a longer con.

- **Watering hole attacks**
    - Channel: websites.
    - Technique: infecting websites that members of an NGO frequently visit with malware to compromise the organisation's systems.
- **Baiting**
    - Channel: physical media or online downloads.
    - Technique: luring victims by promising something enticing in exchange for information or system access. Online, this might be free downloads. Physically, it could be a USB drive labelled "employee salaries."
- **Pretexting**
    - Channel: phone calls, emails, or in-person interactions.
    - Technique: creating a fabricated scenario (pretext) to obtain information from a target. For instance, an attacker might pretend to need certain bits of information from an employee to confirm their identity.
- **Quizzing**
    - Channel: online surveys, emails.
    - Technique: convincing users to answer questions under the guise of a fun quiz, with the actual intention being gathering pieces of personal information.
- **Honey trap**
    - Channel: in-person interactions, online social networks.
    - Technique: an attacker uses romantic or personal allure to obtain sensitive information from the target, either directly or by gaining access to their devices or accounts.

Other common attacks exploit unpatched security vulnerabilities, weak passwords and password reuse, or "plain text" (unencrypted) communication.

<u>Examples of threats and attacks include:</u>

- **Malware and spyware**
    - Channel: malicious software.
    - Technique: designed to infiltrate or damage a device or systems. Spyware specifically aims to gather information about a person or organisation without their knowledge.

- **Ransomware**
  - Channel: malicious software.
  - Technique: once activated, it encrypts the victim's data. Attackers then demand a ransom for the data's decryption.
- **Keylogging**
  - Channel: malicious software or hardware.
  - Technique: a tool used to record a user's keystrokes, capturing everything from passwords to confidential communications.
- **Distributed denial of service (DDoS) attacks**
  - Channel: Internet traffic.
  - Technique: overwhelming a website or online service with traffic to force it to go offline. NGOs might be targeted to silence advocacy efforts or disrupt campaigns.
- **Man-in-the-middle (MitM) attacks**
  - Channel: interception of communication.
  - Technique: attackers secretly intercept and relay communication between two parties. They might eavesdrop or impersonate one of the parties to steal data.
- **Supply chain attacks**
  - Channel: third-party software or hardware.
  - Technique: compromising software or hardware used by the NGO to gain access or disrupt operations.
- **Credential stuffing**
  - Channel: websites.
  - Technique: using automated tools to try a large volume of username/password combinations, often sourced from previous data breaches, to gain unauthorised access.

While physical security is not the primary focus of the guide, it is important to remember that loss and theft of devices (smartphones, tablets, laptops) is still one of the most harmful events for most small organisations.

Note also that risks, threats, and attack techniques evolve. Malicious actors continuously develop new tools and approaches to further their objectives. Examples of emerging threats include AI voice cloning scams ("deepfake audio" used as part of an impersonation fraud), and Internet of Things (IoT) exploits, targeting the large attack surface (and often lax security configuration) of smart devices connected to the Internet.

***Threat modelling***

Threat modelling is a form of risk assessment that focuses on identifying and addressing security threats. It is a structured, usually workshop-based approach used to identify, prioritise, and address cyber risks. This allows NGOs to allocate their limited resources more effectively by focusing on the most significant and likely threats. It also contributes to a clearer understanding of the organisation's security landscape; thus, to better informed decision-making.

Even basic methods, like regular discussions about potential security risks and threats, and brainstorming possible mitigations, can be considered a form of threat modelling. Adopting a simplified, practical approach to threat modelling can still provide benefits, such as improved risk awareness and risk reduction.

# The effects of a data breach

## 2. What are the common impacts of disruption and compromise in the digital space?

When digital systems are disrupted or compromised as a result of a security incident or a data breach, it affects the whole organisation and its external relationships.

- Operations stop: much like a power cut, when digital systems are affected, the affected organisation may not be able to work at all. Even doing basic tasks like sending an email or accessing important documents can be affected.

- Financial loss: repairing and recovering from a digital disruption can cost money. This might include the cost of experts to fix issues, replacing damaged equipment, or potential losses from not being able to operate normally.

- Loss of trust: it takes time and effort to build trust and rapport, but it can be damaged quickly. If partners, beneficiaries, donors, or the wider public don't believe that an organisation can keep information safe, they might choose to work with others instead.

Other potential consequences can include:

- Loss of sensitive information: important and private information might be accessed and taken ("exfiltrated") by unauthorised individuals. This could include details about the organisation, its staff or its partners.

- Damage to beneficiaries: for NGOs, a breach can affect the very people the organisation is trying to help. If sensitive beneficiary information is compromised, this can lead to potential harm to these individuals.

- Impact on staff: staff may feel stressed and overworked as the result of an incident, dealing with the additional tasks and pressures to resolve the issues and restore normal operations.

- Reputational harm: beyond immediate partners, the wider public's opinion of the organisation might be tarnished, affecting the overall reputation of the organisation and its ability to operate effectively in the long term.

- Legal consequences: failure to protect sensitive information, especially personal data may result in fines and lawsuits.

All this disruption, and the resulting potential harm and damage, highlights the importance of preventive actions to protect the organisation, and planning for incident response.

# Knowing value

## 3. What needs protecting?

People, systems, data: at the heart of every organisation is value. Organisations need to know what they have, track their assets, and the risks relating to them; so that an adequate level of protection can be established. Identifying valuable assets (often referred to as "crown jewels") is the first step in better protecting them.

The need to count what they have in their possession motivated ancient societies to develop tools and methods for accounting and bookkeeping. An inherent drive to quantify and keep track of assets and information has led to advancements in mathematics, record-keeping, technology, and even language. These still influence our systems, applications, and processes today.

To coordinate work, organisations need clear lines of communications between their members. As the tools, methods, and objectives of an organisation get more complex, so will the value (and thus the need for protection) of the communications tools themselves increase.

> ***Three pillars: people, systems, data***
>
> People: not only an organisation's own staff, but partners, beneficiaries, and supporters are all essential – their safety and trust is a priority.
>
> Systems: computers, networks, software applications and other technical tools. The engines that drive all digital organisations and enable team members to perform their tasks.
>
> Data: the information transferred, analysed, processed, stored and shared within an organisation, and across organisations. It could be research, personal details, or records of work. Some of this information might be sensitive or confidential.

With that in mind, ask the following questions:

- Which systems and applications are core to day-to-day work for our organisation?
- Have we documented the titles and reporting structures within each function, as well as cross-functional responsibilities?
- What are the essential communication lines that ensure we can work together across teams?
- What types of sensitive data do we handle, and where is it stored?
- Are there non-digital assets, such as paper documents, that also need to be protected?

Every system, software application, data set mentioned in response to these questions is an asset that will require some level of protection. It is similar to taking stock in a shop: create a compact summary of the assets identified through the answers to the above questions. The actual level and means of protection applied to the items on the list – in other words: the investment in securing certain groups of assets – should be proportionate to the anticipated cyber risks and potential impacts of a security incident, as described in the previous two sections. Understanding value is as much about knowing what the organisation has, as it is about understanding how important it is.

## The basics of asset management and creating an asset inventory

- Start simple: make a list of all the important tools, information, and people connected to your organisation.

- Classify by importance: not everything has the same value and importance. Some data might be more sensitive. Some systems might be more critical. Rank them by how vital they are to the organisation. Depending on the volume and types of data handled, some organisations will also develop their data classification policy, data handling protocols, and data labelling processes.

- Assign responsibility: for every asset, there should be a person or a team responsible for its security. This means that someone is always taking care of it.

- Record location: document where each asset is located; be that a physical location (e.g. a laptop on-site in the office or off-site with a remote worker), or in a cloud environment.

- Review regularly: organisations change and grow, and so do their assets. Reviewing the list from time to time ensures it is up-to-date.

***What about remote workers?***

Some organisations reemerged from Covid-19 as remote first, or primarily remote collaboration based. This needs to be taken into account for their security baseline and practices.

- Extended protection: remote workers, being outside the organisation's physical space, interact with the organisation's assets differently. They still access the systems and data, often from varying locations and devices. Thus, the protective measures need to go beyond the organisation's physical boundaries, for example by focusing on protecting accounts/digital identities. See also: *protecting information security while travelling*.

- Secure communication: when working remotely, communication tools become more critical and sensitive. See:

*protecting confidentiality and maintaining integrity.*

- Asset tracking and management: keep track of the devices and tools used by remote workers and ensure those devices and tools meet the general security baseline of the organisation.

- Enhanced awareness: consider extending security awareness communications with messages and advice specifically relevant to navigating the digital workspace in a remote working setup.

- Regular check-ins: consistent communication with remote workers helps to maintain awareness and to share updates on the security practices of the organisation. Also, to address any concerns or queries related to security.

- Emergency response: remote workers should be well-informed and prepared on what steps they have to take in the event of a security incident, ensuring their role in a coordinated response.

# Learning about malicious actors

## 4. Who does the organisation need protecting from?

An introduction to the most common malicious actors and their methods and intentions; e.g. cyber criminals run opportunistic scams via phishing for financial gain, nation-state associated actors orchestrate sophisticated targeted attacks for defamation/manipulation/extortion.

It is important to understand what needs protecting: what is of the highest value owned, managed, processed by an organisation? It is similarly important to understand who they need protecting from.

The most valuable assets and resources (for example the personal data of your donors, or your organisation's own staff members) are expected to be the most likely targets of malicious adversaries. And their attack techniques, motives, perseverance and capacity to act against a target will to a great degree depend on which group of malicious actors they belong to.

The most common threat actor groups are:

- cybercriminals;
- nation-states;
- hacktivists;
- amateurs;
- insiders.

**Cybercriminals** and organised cybercrime is one of the most prevalent dangers online. Their main motivation is financial gain. Therefore, they directly target financial processes (for example by attempting to manipulate payments and money transfers), or data that is easy to sell on underground marketplaces (like credit card details). In other cases they use extortion techniques: utilise ransomware to hold the data of a victim captive, or orchestrate (distributed) denial of services attacks to cause outage and disruption through the overloading of systems. Cybercriminals often engage in opportunistic attacks: like a fisher's dragnet, the volume making up for the lack of targeting and sophistication.

**Nation-state actors** and state-sponsored groups are mostly involved in espionage or disruption that furthers their interests: a sort of "information warfare". They are resourceful and their activities are known to be highly targeted and sophisticated. They often use stealthy methods to obtain access to the target environment, and remain unnoticed within networks and systems, allowing them to observe and gather information on an organisation. This type of actor is also known as advanced persistent threat: complex and hard to detect.

**Hacktivists** (a group that can also include cyberterrorists) are first and foremost ideologically motivated. They are more likely to be constrained in tools and resources, and resort to "loud" (easy to detect) attacks, where

the primary goal is disruption and defamation (while financial gain is their least likely motivation).

**Amateurs**, thrill seekers and so-called "script kiddies": a form of online vandalism. Their main interest only goes as far as testing their skills and tools on easy targets.

**Insiders** (an organisation's own employees, contractors, or partners) are an often overlooked cause of data breaches. As they are already within the organisation with (at least some level of) legitimate access, they easily bypass a number of safeguards and security controls. They may act out of negligence, disgruntlement or for financial gains, potentially in support of other actors from the aforementioned groups

***Hackers?***

Hacker is a word often used in the media to describe perpetrators of cyberattacks, malicious actors, or even security researchers. The origins of modern day hacker culture go back to the computer programmers of the 1960s. A hacker in that context is mostly just someone interested in finding and overcoming the limitations of software and hardware. Such experimentation can result in hacking tools, which in turn can be used both for identifying and fixing weaknesses in networks and systems, or attacking them.

DIY technology enthusiasts maintain community operated hackerspaces (hack-labs, makerspaces) in many cities, and regularly offer workshops on security and privacy topics.

Attributing cyberattacks to specific threat actors with high confidence is a complex task, in many cases only possible with the help of security researchers and government agencies. A list of EU/EEA government organisations providing advice on information security and cyber risk (in the native language of their respective countries) is included in the Appendix.

Even with the uncertainties in identifying malicious actors, it is useful to think about the potential adversaries as it can inform the level of investment into security, or the specific areas (assets, datasets) that have higher protection requirements than others. (See also: *What is the right investment in security?*)

***High profile security incidents from the past years affecting NGOs and civil society actors***

- "Culminating on 16 and 17 April 2023, several media websites in Hungary were targeted with distributed denial-of-service (DDoS) attacks, which temporarily crashed their websites and left readers unable to access news content. Some of the country's leading independent media were among those targeted in the wave of cyber-attacks. Seven media outlets were affected [...] The attacks appeared to have been

coordinated." (source: https://www.mapmf.org/alert/30208)

- In January 2022, humanitarian organisation the International Committee of the Red Cross disclosed that "it has fallen foul of a cyberattack that saw the data of over 515,000 'highly vulnerable people' exposed to an unknown entity. [...] Among the stolen data were names, locations, and contact information." The attack was aimed at a Swiss contractor that stored the data. (source: https://www.theregister.com/2022/01/20/red_cross_hit_by_cyberattack/)

- Red Kite Community Housing, a charitable housing association in the UK has lost £932,000 to a business email compromise (BEC) scam in 2019. "In essence, [the perpetrators] mimicked the domain and email details of known contacts that were providing services to Red Kite. Through this they managed to recreate an email thread that misled those who were copied into the email that it was a genuine follow up to an existing conversation." (source: https://redkite-housing.org.uk/news-blogs/2020/january/we-ve-been-cyber-conned/)

# Protecting the organisation

## 5. What are the essential security measures for cyber hygiene and digital self-defence?

The overarching objective of cyber hygiene and digital self-defence is to establish a stronger security baseline across the organisation. In essence, cyber hygiene is the regular, ongoing practice and application of basic security measures:

- Awareness communication;
- Protecting accounts and account credentials;
- Controlling access;
- Regular patching and upgrading;
- Protecting confidentiality and maintaining integrity;
- Maintaining backups.

This approach also emphasises the importance of aligning security objectives across people, process and technology. Keep in mind: security is not about tools.

***What is the right investment in security?***

Getting security spending right is a complex task with many variables. One of the overall objectives of this guide is to give tools and pointers for a balanced approach to security investment. However, it cannot be a substitute for each organisation doing their own analysis and planning. Combine methods described in the different sections of the guide to drive an internal discussion, and have an informed decision on budgeting for security.

- Risk assessment and threat modelling – which of the cyber risks are most relevant to the organisation?
- Awareness communication on cyber hygiene and digital self-defence – are staff members regularly briefed on security requirements applicable to them?
- Prioritisation of essential security measures – which protection technique is the most relevant in the given context?
- Continuous improvement – can the organisation develop a security roadmap and implement measures in a phased approach?
- Legal and regulatory compliance – could the organisation be exposed to a fine due to non-compliance?
- External support and funding – are there grants available for security improvements, non-profit discounts from software vendors or consultancies offering pro bono work?
- Surveys and forums – can you seek and access input from peers?

For a rough benchmark across different sectors and industries, consider 10–15% of the technology and IT budget, or 1–3% of the operating budget as an average amount allocated to information security. Nonetheless, even that amount is a significant commitment for organisations with constrained resources. Once again, this highlights the value of inexpensive (or even free) options, like practising good cyber hygiene. Improving security culture and cyber-conscious behaviour can be the most cost-effective, high-impact measure to secure information.

## Awareness communication

The same way basic health and safety practices are critical to preventing accidents and diseases in a physical environment, security awareness is essential to preventing security incidents and data breaches in the digital domain. Think of cyber hygiene as the information security equivalent of the simple act of handwashing: a basic and highly effective practice for prevention.

Just as handwashing requires basic knowledge and awareness about its importance (think of messaging during a pandemic), simple security awareness communication can inform users about cyber risks and the basic practices to mitigate them.

- Publish an internal statement on information security, bringing attention to the importance of the topic, and setting a baseline for all staff members, contractors, and partners (see Appendix for template).

- Utilise freely available online resources, tutorials and toolkits to share security awareness messages and to educate staff on digital self-defence. Take and share sections from this publication as a start.

- Integrate basic awareness communication into existing training programs like the induction process. This can ensure that staff members receive essential security information with minimum time investment.

- Concise, focused and relevant security tips delivered frequently are better than long sessions.

- Encourage staff to be vigilant and promote a culture of security. Consider appointing security champions in each team (see: Continuous improvement of the security posture).

Extensive training and education on information security and cyber risk is common practice in larger corporations as part of their compliance regime. This is often not feasible for smaller teams. Regardless, there are plenty of free resources to leverage in case the organisation decides to extend their security awareness activities (see Appendix for a list of government organisations, as well as independent

privacy and security advocacy groups offering guidance and advice). Notably, this can be important following a security incident or a "near miss", to help the organisation recover more quickly, and ensure a safer posture going forward.

## Protecting accounts and account credentials

People and organisations connect to and engage with Internet services using their digital identities. These digital identities are mostly based on email accounts. Thus, not all accounts are created equal. Using work email and password "123456" to download a free research paper is a different risk than using the same email address and "secret password" to register for a conference, or to access an organisation's Microsoft 365, Google Workspace (including Gmail), Slack, Asana, Basecamp, Miro, or a similar system that is core to productivity and daily work, to collaborate with colleagues or to coordinate external partners.

***Key cyber-conscious habits to safeguard accounts and digital IDs:***

- use strong, complex passwords,
- avoid reuse of the same secret (password) for multiple accounts,
- do not share credentials (username/ID, password, tokens, one-time authorization code, etc.) for individual accounts,
- share secrets to group IDs (shared accounts) using a secure mechanism (for example a password manager),
- enforce multi-factor authentication,
- consider going passwordless using passkeys,
- evaluate the necessity for hardware keys,
- implement additional measures for high risk users,
- consider additional protection for administrator IDs and privileged accounts,
- immediately change credentials in case there is indication of a compromise (for example, a password was disclosed in a data breach).

***What constitutes a complex password?***

A complex password (or strong password) is one that is designed to be difficult for others to guess or decipher ("crack"). It is critical to securing accounts. A complex password:

consists of at least 12 characters (the longer, the stronger);

combines uppercase and lowercase letters, numbers and special characters (ideally at least three out of the four categories);

avoids common words and combinations ("password123"), or even seems random in its composition;

does not include references to the user like their birthday, name or other information that could be easily obtained by others,

is unique to each site and service, and distinct from previously used passwords.

***Multi-factor authentication (MFA)***

Think of different types of bike locks: a d-lock, steel chain, folding lock, frame lock. Each represents a different level of security and requires different tools to be picked or forcefully removed. When concerned about an expensive bike getting stolen, it is best to lock it with multiple locks, ideally using different types of locks.

MFA (and its variations, like Google's "2-Step Verification") is a security mechanism that requires users to verify their identity by providing multiple pieces of evidence or factors before granting access. Typically, it involves at least two of the following: something the user knows (password), something they have (security token or phone) and something they are (biometric verification).

The purpose of MFA is to add an extra layer of security, making it harder for attackers to gain access even if they have the username and password. By requiring multiple verification methods, it significantly reduces the risk of unauthorised access. Implementing MFA is a crucial and cost-effective way to enhance security.

Keep in mind: if your organisation and users are new to the concept of MFA, its implementation and roll out should be supported by clear communication and education.

***The use case for password managers***

Password managers store and manage credentials (primarily usernames and passwords) in a secure vault and make them accessible across multiple devices. They make it easier to use unique, complex passwords for each service without needing to remember them all. They usually require one strong master password to access the stored passwords and can often generate strong (random) passwords for the user.

Several Internet browsers and operating systems now have a basic password manager integrated. For most small organisations, it can be sufficient to instruct users to use Google Password Manager in Google Chrome (to generate, save, and fill in user credentials), or to use the iCloud

Keychain if they primarily work with Apple devices.

Enterprise grade password managers also allow for secure sharing of credentials among team members with robust encryption, audit logs and role-based access controls. (See also: specific examples of password managers mentioned under Protecting confidentiality and maintaining integrity.)

In addition, some password managers will have a feature to detect passwords that were compromised in a data breach and subsequently published in a public data dump.

***Pay attention: high risk users, administrator IDs and privileged accounts***

Leaders, decision makers, core influencers of an organisation can be considered high risk users, as hijacking or spoofing (impersonating) their accounts can be used in social engineering scenarios. Think of the immediate emotional impact of an email with the subject "urgent!" if it appears to be coming from the boss of your boss.

Administrator accounts yield high privileges over systems and their configuration. Someone overtaking the account of the sole IT person will have the power to cause serious disruptions in the daily operations of the organisation. Alternatively, a malicious actor may lay dormant to observe and analyse the data they can now access. Such behaviour can prepare the ground for a man-in-the-middle (MitM) or eavesdropping attack, which in turn can result in access to other systems. Over time, such attack behaviour (known as advanced persistent threat, or APT for short) can undermine the integrity of communications within the organisation. This ultimately will also erode overall trustworthiness.

## Controlling access

Keeping accounts and digital IDs safe and secure (a key requirement for the act of "authentication") is only half the battle. It's similarly important to control which systems an account can access ("authorisation"), and what an account can view or change within a system they have access to ("privilege management").

Controlling access and managing privileges effectively are fundamental to safeguarding data and systems. A streamlined and straightforward approach, focusing on essential actions, can help in managing access without the need for complex processes or lengthy policies. From a human resources perspective, the access lifecycle is the digital counterpart to joiners, movers, leavers (JML) processes.

***Onboarding checklist***

- Create user accounts with minimum required privilege: only assign the level of access (or permissions) needed for the new team member to accomplish their tasks.
- Implement a password policy (configure minimum complexity requirements) where possible.
- Enforce password change upon first login.
- Enable multi-factor authentication (MFA) where possible.
- Provide information on secure access practices and password management.

***Regular access review checklist***

- Periodically review user account privileges and adjust access levels based on current roles and responsibilities. (*Note*: a regularity of 6–12 months is a good guideline, depending on the size of the organisation and the frequency of change of team members and systems.)
- Deactivate accounts that are no longer needed or in use. (*Note*: this can also save costs on software subscriptions and licences!)
- Confirm that MFA is active on all possible accounts and systems.

***Offboarding checklist***

- Promptly deactivate or delete user accounts of leavers.
- Change shared passwords that the leaver had access to.
- Retrieve all assets from the departing team member.
- Remind departing members of confidentiality obligations as part of their exit interview.
- Review and update access privileges to sensitive information and systems.

***Incident response workflow***

- In case of suspected unauthorised access or account compromise, immediately change passwords and enforce logoff across all devices.
- Investigate the incident to determine the extent and impact – see *Incident response and recovery* for further details.

Further considerations for larger teams and more complex systems:

- Implement role-based access control (RBAC): define access permissions based on roles within the organisation, ensuring users have access only to the resources necessary for their role. Most systems and applications offer a "group"

or "organisational unit" (OU) structure to enable RBAC.

- Where possible, enable access logs. Keeping logs of who accessed what and when provides an audit trail that can be crucial for investigations in case of a security incident.

***Controlling access to social media accounts – protecting online presence***

Securing social media accounts is crucial for small organisations to protect their online presence and reputation. Consider general advice from the "Protecting accounts and account credentials" and "Controlling access" sections, and pay extra attention to the following:

- the use of strong passwords and enabling MFA (to protect against credential stuffing and other brute force attacks) is even more important due to the increased exposure;
- limit access to necessary personnel only, and consider the differences in the access models of each platform (for example: being a group admin or moderator for Facebook, or possessing the credentials for an X/Twitter account);
- monitor account activity, if possible create some alert mechanism for the prompt detection of account hijack;
- configure recovery email addresses and phone numbers to regain access quickly in case of an account take-over/lockout;
- limit the use of third-party apps and services connected to social media, regularly review and revoke unnecessary permissions.

One more note: similar considerations can also apply to the official website of the organisation.

## Regular patching and upgrading

Writing software systems and applications without bugs and errors is a hard task. This is the result of the inherent complexities of today's computer technology. Hardware is also impacted by the same intrinsic flaws, as it is controlled by small pieces of computer code (think "firmware"), and requires an intermediary layer of software (like the "operating system") to run the apps we know, and to enable access to online services we require for communication and other aspects of our daily work. Some of these bugs can lead to security vulnerabilities. These vulnerabilities in turn become threats and cyber risks, if they remain unaddressed. Therefore, regular patching and upgrading is an unavoidable reality for all of us.

Practical steps:

- **Automate updates**: enable automatic updates wherever possible to ensure that software and applications are always up-to-date. Remind users not to turn off or block these automatic updates.

- **Prioritise critical updates**: pay immediate attention to critical security updates and patches that fix severe vulnerabilities. Alert staff to let their app/system update, and reboot their devices when needed.

- **Schedule regular maintenance**: depending on the types of systems in use, IT administrators may have to allocate specific times for performing system updates and maintenance to avoid disruptions in daily operations. Affected users should be made aware of possible downtime. Ideally this can happen outside core office hours.

- **Keep inventories**: maintain a list of all software and hardware in use and regularly review it to ensure that all items are up-to-date and still supported by vendors. (See also: The basics of asset management and creating an asset inventory.)

- **Monitor for vulnerabilities**: stay informed about newly discovered vulnerabilities related to the tools and technologies used by the organisation. Most vendors offer official channels (for example email newsletters) for such topics. Note: this is less of a concern for primarily cloud-based organisations, although they should still pay attention to updates from the maker(s) of the operating system(s) running on the devices of staff members.

***The real reason for patching: software without flaws is hard to do – and this impacts security***

Creating error-free software is a nearly unattainable goal for a number of reasons.

- Inherently complex interactions: multiple components and systems interacting can lead to unpredictable and unintended behaviours, making the identification and resolution of potential issues a highly complex task.

- Changing user requirements: alterations and additions to initial requirements can create inconsistencies and new points of failure, resulting in continuous revisions and adaptations of the software.

- Variable operating conditions: diverse hardware, network configurations, and user interactions can affect software operation, potentially revealing latent issues under specific conditions only.

- Dynamic and unpredictable environments: the continuous evolution of technology and the introduction of new development frameworks and

standards can generate unforeseen incompatibilities and issues.

- Uncertain information on external dependencies: reliance on third-party services, libraries, or components, which might be imperfectly understood or documented (or not well maintained), can introduce errors and vulnerabilities throughout a whole chain of interdependent software.

- Impracticality of exhaustive validation: the seemingly infinite possible states and interactions within software make comprehensive testing and validation unfeasible, allowing some bugs (for example so called "edge cases") to remain undetected.

## *Protecting confidentiality and maintaining integrity*

Cryptography is the science and application of "secret writing" (from new Latin "crypto-" meaning covered, or hidden). In the digital domain, and in the context of information security this translates to encryption (encoding) and decryption (decoding) of messages and data.

Encryption tools and techniques are core to two principles ("tenets") of security: confidentiality and integrity. On a high level, when implementing encryption for confidentiality, it means shielding sensitive data from unauthorised access by making it unreadable, while integrity means protecting the data from alterations. Cryptography is essential for maintaining digital trust and the compliance of digital systems.

Important applications of cryptography include:

- **Secure communication**: cryptography protects the confidentiality and integrity of information during transmission, ensuring secure communication between parties.

- **Data security**: encrypting data at rest protects sensitive information stored in databases, files, or storage devices against unauthorised access.

- **Authentication**: cryptographic protocols play a role in verifying the identity of users, systems and applications, ensuring that they are who they claim to be.

- **Digital signatures**: cryptographic hashing algorithms provide a way to confirm the origin and integrity of digital messages or documents, acting as a digital "seal of authenticity".

Cryptography and encryption tools are a rabbit hole within the security industry and among privacy and data protection enthusiasts. It's a very technology heavy topic, that also requires some degree of interest in mathematics and engineering (for example to have meaningful conversations on symmetric vs. asymmetric

cryptography). For the intents and purposes of this guide, it's recommended that NGOs have awareness of the tools and solutions below. (Note: this list is not meant to be exhaustive.)

Practical use of encryption:

- **Device encryption**: activate full disk encryption available in operating systems; like BitLocker for Windows, FileVault for macOS and encrypting file systems in Linux.

- **Email encryption**: use email platforms that offer built-in encryption like ProtonMail or leverage encryption features in mainstream platforms like Outlook.

- **Secure messaging apps**: opt for messaging apps with end-to-end encryption (E2EE), such as Signal (https://signal.org/), Element (https://element.io/), or Wire (https://wire.com/) for secure, confidential conversations.

- **VPN services**: use Virtual Private Networks (VPN) to encrypt internet traffic, especially when the use of unsecured Wi-Fi networks cannot be avoided.

- **Secure cloud storage, secure file sharing**: choose cloud storage services offering automatic encryption like Dropbox (https://www.dropbox.com/) or Tresorit (https://tresorit.com/) for storing and sharing documents securely.

- Password managers: use reputable password managers like 1Password (https://1password.com/) or Bitwarden (https://bitwarden.com/), which use encryption to securely store and manage login credentials. (See also: *The use case for password managers*)

Encrypted data transfer: use methods with encryption, like HTTPS when accessing websites or SFTP for file uploads and downloads.

***Point of view: private ways of browsing the Internet***

Some of the security tools and techniques mentioned in this guide will help to enhance privacy online and reduce the risk of unwanted data collection and surveillance. However, the connection is less clear in the opposite direction: privacy preserving methods for browsing won't necessarily improve the overall security posture of an organisation (except under specific circumstances, for example a threat model that assumes the need for protection against surveillance, and in case all members of the organisation consistently use the same privacy-focused tools and methods).

Pointers for more detail on online privacy:

- privacy-focused browsers to block tracking (examples: Brave, Tor, Firefox) – privacy and security enhancing browser extensions/add-ons also exist but have a limited scope and use case;

- privacy respecting search engines that do not store or track personal data (examples: DuckDuckGo, Startpage);

- virtual private network (VPN) tools that encrypt communication and mask the source address (examples: too many, but most of the above providers also offer VPN solutions).

A note on the limited nature of the "private"/incognito mode of popular browsers: this is a mode where browsing history, passwords, and other private data are not saved. This can be useful for having a "fresh session" (for example on a shared device) or temporarily avoiding tracking by websites. However, it doesn't provide anonymity and neither does it hide the browsing activity. Think of it more like a tent or portable cabin for changing on the beach.

(A side note on terminology: while "crypto currencies" use forms of cryptographic mechanisms, they have no direct relevance to information security, cyber risk, or the adjacent concepts as they are discussed in this publication.)

## Maintaining backups

Regular backups are crucial for recovery from data loss incidents, ransomware attacks or system failures. It is also critical to secure backups, regularly test restoration processes, and store backup copies in a separate, secure location. All this is primarily a task for IT or the organisation's technology vendors. However, staff members may have to take responsibility for having backups of data locally stored on their devices, or always working online to ensure up-to-date copies of their work are stored in internal systems.

Essential considerations for maintaining backups include:

- Type and variety – full, incremental, and differential backups have different purposes.

- Frequency – the schedule of when different types of backups are created for each system.

- Security – securing backups with encryption and robust access controls to protect them from unauthorised access or alterations.

- Testing – verifying restoration processes to ensure data can be successfully recovered when needed.

- Storage – multiple physical locations or reputable cloud services.

Also consider the need for **secure data disposal**: when data, and a corresponding backup is no longer required, securely delete or dispose of it to prevent unauthorised access or disclosure. Methods may include secure file deletion tools or shredding of physical documents. **Data retention** periods play a part here: disposing of certain records or data sets can be mandatory to meet legal and regulatory compliance.

*A note on Software as a Service (SaaS)*: many organisations use SaaS applications like Google Workspace, Microsoft 365 or Salesforce, assuming that their data is automatically protected and backed up by the service provider. While these providers do have robust measures for resilience (including redundant storage and extensive backup regimes), organisations can and should take responsibility for their own data backup. Where applicable, check settings and options relating to backups in the SaaS provider's system. Assess the risk: if necessary, consider using third-party backup solutions specifically designed for SaaS applications to have more control and flexibility over backups.

***Template: protecting information security while travelling***

Remote working presents unique security risks. To increase awareness of some of the challenges, create a short guide with the following points and distribute it to all staff.

- **Only connect to secure wireless networks** – Open Wi-Fi is a hacker's playground. Avoid connecting to open (passwordless) or public Wi-Fi networks. Consider tethering data from a smartphone (if unlimited mobile data is available). If the use of public Wi-Fi is unavoidable, ensure that the hotspot (wireless access point) belongs to a legitimate provider, and isn't a rogue one; for example, double check that the name of the wireless network is exactly the same as the one advertised on signs, and not one with typos. If necessary, ask staff for help.

- **Physical security of devices** – Don't leave devices unattended: use hotel safes, lock them in the luggage. When using a laptop lock (Kensington Lock), double check that the device is secured properly before leaving it unattended.

- **Always lock the screen** – In the exceptional cases you do leave a device unattended (and preferably secured with a lock as per the previous point), make sure you lock the screen, so that the contents of the display cannot be read, and the device cannot be accessed in your absence.

- **Ensure devices are password protected** – All your devices (laptop, smartphone, tablet, etc.) should have a PIN, password, pattern lock, biometrics, hardware key, etc.

- **Report lost or stolen devices** – Important in general, but even more a risk while travelling. All members of the organisation should be aware of the way of making a report without access to internal resources (for example by sending an email from an external address). Stolen devices should be reported at a local police station also. (This will be necessary when claiming insurance.)

**Be aware of shoulder surfing** – Always be aware of your surroundings. Be cautious when entering passwords. Be wary of strangers taking undue interest in the screen: they might be trying to initiate a conversation to extract information. Consider the use of a privacy screen protector.

**Limit confidential discussions** – Be mindful of where and when work matters are discussed. Public places are not ideal for confidential talk: save secrets for safe spaces.

**Cross-border travel** – When travelling internationally, in some countries customs officers might request access to visitors' laptops, smartphones and tablets. While it may be legally required to submit to a device inspection, it should be possible to decline providing passwords to online work accounts.

# Incident response and recovery

## 6. How to work towards resilience?

Most organisations cannot completely escape becoming the victim of some form of cyberattack or security compromise at some point in time. It is important to be able to detect such incidents, to be able to react to them and to recover from them. In some cases this will also include informing members, partner organisations, the authorities or even the general public. Preparing the lines of communication and clear messages will help to reduce negative impact, and thus improve resilience.

Even a simple plan will help. For instance, including the reporting line for security incidents in the organisation's *information security statement* (see Appendix – Template: statement on information security). Proactive, upfront investment in security should help reduce the fallout and costs of an incident.

The critical questions to ask:

- Do all people in the organisation know how to detect an incident?
- Do all people who detected an incident know how they can report it before they react?
- Do external partners have a channel for reporting incidents?
- What happens once someone reports a security incident?
- Who is responsible for managing and coordinating the incident response process?

The following four steps explore the details.

## Detection and validation

Not all suspicious activities are security events, not every security event is a security incident, and not every security incident will result in a data breach.

- Suspicious activities are notifications and "warning signs" that should be checked and validated.
- A security event is when a "warning sign" is proven valid but not necessarily harmful.
- A security incident is when there is real and potential harm, but it can be contained.
- A data breach is when the harm has resulted in unauthorised access, loss or disclosure of data.

The ability to detect suspicious activities is the first step in this process. Large corporations often build their own Security Operations Centre (SOC), or engage a Managed Detection and Response (MDR) or Managed Security Service Provider (MSSP) vendor for this purpose. These solutions are not just expensive and resource intensive, but often unnecessary for small organisations.

In case of limited resources and know-how, relying on the vigilance of staff members and maximising the use of existing tools is crucial for detecting unusual or unauthorised activities.

- Train all members of the organisation to recognise potential security incidents, such as phishing attempts. Encourage them to report these promptly.

- Most cloud computing, productivity, and collaboration tools come with built-in security features and alerts. Empower a member of staff to familiarise themselves with these features.

- Configure notifications and check alert settings in tools to ensure that the right people get informed immediately.

- Review account activity on a regular basis: where available, check the activity logs provided by the apps, systems and cloud services in use.

In organisations with small teams and flat hierarchies, having clear and simple reporting mechanisms is key. Everyone should feel comfortable and responsible for reporting security concerns, and information should be quickly and effectively shared among all members.

- Create a simple reporting form or channel: an accessible and straightforward way for team members to report concerns. This could simply be a dedicated email account. Productivity, and collaboration tools already in use may also offer a convenient option; consider service desk tickets for example.

- Designate a go-to person: the main contact for any security concerns or incidents, ideally someone with knowledge of digital tools and security. They get alerted via the reporting form/channel.

- Have a backup: a second person should be designated as a backup in case the main contact is unavailable. Alerts and reports via the form should be automatically routed to them in case the primary person is not available.

## *Incident management and containment*

Incident response planning is like having a map when you go hiking: it shows the way in case you get lost. Once a security incident has been reported and validated, clear communication helps in reducing confusion and panic and ensures that the right steps are taken timely. This helps in managing and containing security incidents before they can escalate.

Consider the following steps:

- **Appoint an incident management tea**m
    - Having a designated team brings organisation and structure to the incident response process. (This can consist of existing staff members.)
    - Key areas of responsibilities in this team should cover: manager/coordinator, security analyst, IT specialist, communication specialist, legal counsel, scribe/documentation specialist.
- **Assess the scope and impact**
    - Identify the nature and breadth of the breach, such as the types of data involved and the number of individuals affected.
    - Assess the risk associated with the breach, considering the sensitivity of the compromised data and potential consequences.
- **Document and preserve**
    - Maintain detailed records: document every action taken, from detection to containment, ensuring a clear and chronological record of the event and response actions.
    - Preserve evidence: collect and preserve any evidence related to the security event for further analysis and potential legal actions. Depending on the severity, this may require the help of a Digital Forensics and Incident Response (DFIR) specialist.

The incident management team should decide who needs to know about the incident. In small organisations, this could mean keeping the whole team informed about the status of any ongoing security concerns. Explain the steps being taken to address the issue. Regular updates help maintain trust and ensure that everyone is on the same page.

## *Data breach response*

Once the incident management team confirms that the incident resulted in unauthorised access, loss or disclosure of data (rather than being a false alarm or a “near miss”), the next steps revolve around communication and immediate actions to mitigate damage.

Follow the checklist:

- **Immediate containment**
    - Disable compromised user accounts and reset passwords for affected users. In some cases, it can be safer to enforce a password reset for all accounts. Remember to inform affected team members, including remote staff, so that nobody gets locked out of work.
    - Isolate affected systems to contain the breach and prevent further unauthorised access or leakage of information.

- **Notification of impacted parties and external communication**
    - Notify the affected partners and individuals. Explain the nature of the breach, the type of data involved, steps you have taken to remediate the breach, and steps they can take to protect themselves.
    - If applicable, report the breach to the relevant authorities, complying with legal and regulatory requirements like GDPR.
    - Evaluate options and strategies for public communication; for example using the organisation's official website, social media channels, or informing media outlets.
- **Investigation**
    - Conduct a review to understand how the incident happened. Gather and document evidence.
    - Maintain a clear record (incident log) for future reference and compliance.
- **Mitigation and remediation**
    - Consider if measures should be implemented to mitigate further impact of the incident.
    - Remediate the vulnerabilities that led to the breach. Reinforce security controls to prevent future occurrences.

***Notification of a personal data breach to the supervisory authority***

Remember: if your organisation needs to comply with the EU's General Data Protection Regulation (GDPR), as per Article 33(1), your organisation "shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay." (source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679)

Examples of personal data include name and surname, home address, email address such as name.surname@company.com, identification card number, and more. (source: https://www.consilium.europa.eu/en/policies/data-protection/) Please seek further guidance from your local data protection authority; see list under https://edpb.europa.eu/about-edpb/about-edpb/members_en

***Point of view: communication to media***

Informing the media of a security incident is a significant step. Nonetheless, it is often necessary in case of a substantial public interest or impact. Accepting re-

sponsibility for the breach, and offering a genuine apology to the affected parties can help to rebuild trust.

- **Prepare a communication strategy**
    - Prepare messages that are transparent, factual and empathetic. Avoid speculation, blame or overly technical language.
- **Consider the timing**
    - Wait to see if the media contacts the organisation can be risky, as it may lead to the spread of speculation or misinformation.
    - Early, proactive communication can help manage stakeholder expectations and trust. Communicate as soon as you have verified information, even if the full picture is not yet clear.
- **Release information in a controlled and coordinated manner**
    - Designate a trained spokesperson to handle media inquiries and ensure consistent messaging. Consider providing regular updates.
    - While transparency is key, avoid disclosing details that could compromise the ongoing investigation or the security of the systems involved.
- **Open lines of communication**
    - Create a channel for affected parties to ask questions, seek clarifications, and obtain support.

## *Recovery and improvement*

After managing the immediate impacts of an incident and a possible data breach, the organisation should focus on recovering and learning from the incident to enhance future resilience.

Key steps include:

- **Restore normal operations**
    - Monitor systems for signs of anomalies or malicious activities to ensure that the mitigation and remediation steps were successful.
- **Implement lessons learnt**
    - Reflect on the investigation and identify the root causes, and the effectiveness of the response.
    - Modify security measures to address identified shortcomings. If necessary, implement new safeguards.

- **Continuous improvement**

  - Review and update the incident response plan, reporting mechanisms and communication protocols to ensure their effectiveness.

  - Use the insights gained from the incident to improve security awareness communication.

***Useful reference: Incident Handler's Handbook***

The most widely implemented framework for incident response is the SANS Institute's Incident Handler's Handbook. The four steps in this section can be considered a condensed version of their six step approach:

1. Preparation;
2. Identification;
3. Containment;
4. Eradication;
5. Recovery;
6. Lessons learned.

Be prepared: in case of a powerful adversary (nation state actor or pervasive cyber criminals) and a severe incident, most organisations do not have the internal resources and experience to manage the situation on their own and need to bring in external experts to support one or more of the above steps. This is especially true when a criminal investigation is required, and forensic evidence needs to be collected (which usually requires engaging a DFIR specialist).

# Continuous improvement of the security posture

## 7.Why even the best protected organisations must stay vigilant?

For many organisations, the ability to operate without disruption is crucial. Ensuring that security processes operate adequately is a vital part of business continuity planning. The cost of a security incident (downtime, remediation efforts, potential fines) can be significant. Even small ongoing investments in regular awareness reminders and practising cyber hygiene is more cost-effective than dealing with the aftermath of a breach.

A healthy dose of paranoia and scepticism can be turned into vigilance and critical analysis to drive the continuous improvement of the security posture. Even with extensive awareness training and advanced security systems in place, human error remains a significant factor. Staying perceptive and applying critical thinking will help reduce the occurrence and impact of such errors and mistakes.

Appointing security champions can significantly benefit an organisation's information security posture. A security champion is typically an individual from a non-security team who has an interest in security. This person acts as a bridge between the security team and other departments, ensuring that security best practices are followed in all areas of the organisation.

With the help of security champions, organisations can:

- Embed security in all teams and functions;
- Rely on peer training and knowledge sharing to improve security awareness;
- Improve communication on information security and cyber risk topics;
- Impact cultural change towards cyber-conscious behaviour;
- Create a feedback loop on the implementation of security practices;
- Have points of escalation for reporting suspicious activities and security incidents.

**Security is a process:** it is never over, it is never done. Adversaries improve, threats change, attack techniques evolve – and so must organisations continually adapt and develop their capabilities to withstand unwanted disruptions.

# Appendix

## Glossary

| Term | Definition |
|---|---|
| Access control | A method of restricting access to resources, enabling permissions to be allocated to users, groups or roles. |
| Advanced persistent threat (APT) | A prolonged and targeted cyberattack seeking to access and potentially harm an organisation's resources, often remaining undetected for a period. |
| Allowlist | Also known as "whitelist", a list of "safe" items, individuals or entities that are explicitly allowed or granted access, privileges or recognition, ensuring that only approved and trusted actions or interactions are permitted. The opposite of a blocklist. |
| Antivirus software | Programs designed to detect and eliminate malicious software, such as viruses and malware, from computers or networks. |
| Application security | Measures taken to improve the security of an application (from mobile apps to complex IT systems) often by finding, fixing and preventing security vulnerabilities. |
| Asset inventory | A compiled list of an organisation's resources including software, hardware, and information. |
| Authentication | Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in a system. |
| Authorisation | The process of granting or denying access to a network or system, which allows the user different levels of access to various resources based on their identity. |
| Backup and recovery | A copy of data or software, and the tools and procedures that allow a system to be restored following a data loss event. |
| Biometrics | A method of verifying an individual's identity based on unique physical or behavioural characteristics, such as fingerprints, facial recognition or voice patterns. This form of identification may provide an additional layer of security and can be used for accessing devices or systems. |

| Term | Definition |
|---|---|
| Blocklist | Also know as "blacklist", a list of entities that are blocked or denied privileges or access (most often as they are known to be malicious). The opposite of an allowlist. |
| Botnet | A collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by malware. |
| Browser cookies | Small pieces of data stored by websites in a browser, often used to keep track of user activities and preferences. |
| Business continuity planning (BCP) | A process involving the development and implementation of a plan to help continue operations in case of serious incidents or disasters and to recover to an operational state within a reasonably short period. |
| CIA triad (Confidentiality, integrity, availability) | A security model designed to guide policies for information security within an organisation. |
| Cloud security | A set of procedures and technologies that work together to protect cloud-based systems, data and infrastructure. |
| Credentials | Usernames, passwords, and other methods used to confirm a user's identity for authentication and authorisation purposes. |
| Cryptography | The practice and study of encrypting information, to secure communications and sensitive data, such as passwords and personal information, and to validate the authenticity of messages or documents. |
| Cyberattack | An attempt by individuals or groups (threat actors) to damage, disrupt or gain unauthorised access to computer systems, networks or data, typically via the Internet. |
| Cyber-conscious | Awareness and understanding of cyber risks and applying practical methods for cyber hygiene and digital self-defence. |
| Cyber hygiene | Habits, routines and steps taken by users to improve online security. |
| Cyber resilience | An organisation's capability to prepare and respond to (attempted) cyberattacks and recover after a security incident occurs. |
| Cyber risk | The potential of loss or harm occurring to an organisation's information systems and data, due to vulnerabilities, threats or cyberattacks. |
| Cybersecurity | A subdomain of information security, the practice of protecting systems, networks and applications from cyberattacks. |
| Data availability | Part of the CIA triad, ensuring that data is accessible when needed by those who need it. |
| Data breach | A security incident where unauthorised access is gained to confidential data. |
| Data confidentiality | Part of the CIA triad, the practice of keeping information secret and accessible only to authorised entities. A core component of security. |

| Term | Definition |
|---|---|
| Data disclosure | Releasing data, intentionally or unintentionally, to untrusted environments. |
| Data encryption | The process of converting data into a code (ciphertext ) to prevent unauthorised access. |
| Data exfiltration | Unauthorised copying, transfer or retrieval of data from a computer or server, a form of data breach or data disclosure. |
| Data integrity | Part of the CIA triad, maintaining and assuring the accuracy and consistency of data over its entire lifecycle. |
| Data loss | The unforeseen loss of data or information, often due to damage, deletion or corruption, resulting from a security incident. |
| Data loss prevention (DLP) | Strategies, solutions and tools to ensure the prevention of data loss or leakage. |
| Data protection | Measures and practices to safeguard against security compromise or data loss. Crucial for maintaining the privacy of individuals, and often involves compliance with laws and regulations to avoid legal repercussions. |
| Data Protection Officer (DPO) | A role within a company responsible for ensuring that data protection activities are compliant with relevant laws; for example, the EU's General Data Protection Regulation (GDPR). |
| Data retention | The practice of storing records for set periods, ensuring they are accessible when needed, such as audits, or compliance purposes. The duration and method of retention may vary depending on the type of data and applicable laws or organisational policies. |
| Data, information | Representations of facts, statistics or descriptions of objects, expressed in any medium, that can be read, processed, transformed, etc. by humans or machines. |
| Database security | Various measures aimed at protecting databases and database management systems against compromises of their integrity, confidentiality and availability. |
| Device encryption | The practice of converting the information stored on a device into a format that can't be read without the correct password or encryption key. |
| Digital Forensics and Incident Response (DFIR) | Methodology used to approach and manage security incidents and data breaches. Digital forensics specifically involves the collection and analysis of electronic evidence, to uncover what happened during an incident, and for potential legal proceedings. |

| Term | Definition |
|---|---|
| Digital identity | A body of information about an individual, organisation or device that exists online. |
| Digital self-defence | Protective measures individuals and organisations can take to secure their information online and maintain digital safety. |
| Digital signature | A mathematical scheme and corresponding tools for verifying the authenticity of digital messages or documents. |
| Digital trust | The confidence users have in the ability of people, technology and processes (or a specific organisation) to create a secure online environment and digital products. |
| Disaster recovery plan (DRP) | A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Often part of business continuity planning (BCP). |
| Distributed denial of service (DDoS) | A type of cyberattack where multiple (compromised) systems are used to target a single system causing an outage, typically through overload of the target system. |
| Email encryption | The process of encrypting the content of an email message to protect it from unauthorised viewing and modification. |
| Email filtering | The process of allowing software to categorise, organise or block incoming email, based on predetermined criteria. For example to prevent or reduce spam and phishing. |
| Encryption | The method by which information is converted (encoded) into a secret code (ciphertext ) that hides the information's true meaning. |
| Encryption key | A piece of information that is used to encode or decode data. |
| Endpoint detection and response (EDR) | Solutions that focus on detecting, investigating and mitigating suspicious activities on hosts and endpoints. |
| Endpoint security | Practices and software used to protect end-user devices (like laptops and smartphones) from being compromised by malicious actors. |
| End-user protection | Security measures designed to protect individuals against a range of threats, securing their digital experiences. |
| Facial recognition | A biometric software application meant for uniquely identifying or verifying a person by comparing and analysing patterns based on the person's facial contours. |
| Fear, uncertainty and doubt (FUD) | A disinformation strategy used in sales, marketing, public relations, politics and propaganda to influence perception. Also used by some vendors in the cybersecurity industry to motivate higher spending on security tooling and services. |

| Term | Definition |
|---|---|
| Firewall | A security device (or software) that monitors and filters incoming and outgoing network traffic based on an organisation's previously established security policies. |
| Firmware | Class of computer software that provides low-level control for the specific hardware component of a device. |
| General Data Protection Regulation (GDPR) | A regulation in EU law on data protection and privacy in the European Union and the European Economic Area. |
| Hacker | Member of a subculture of tinkerers, makers and technology enthusiasts with broad and varied sets of skills and interests. Some have benign motivations to push the limitations of a technology, others are operating as threat actors. |
| Honeypot | A computer security mechanism set to detect or deflect attempts at unauthorised use of information systems. |
| Identity and Access Management (IAM) | A framework for business processes that facilitates the management of electronic or digital identities. |
| Identity theft | The unauthorised use of someone's personal data, usually for financial gain. |
| Incident management | The activities of an organisation to identify, analyse and remediate a security incident, and to prevent a future recurrence. |
| Incident response plan | A structured approach detailing the steps to follow when a security incident occurs. |
| Incident response team | Members of an organisation responsible for managing and mitigating security incidents. |
| Information security (InfoSec) | The practice of protecting data from unauthorised access, disclosure, alteration or destruction, and maintaining the confidentiality, integrity and availability of information. |
| Internet of things (IoT) | A system of interrelated devices that are connected to the Internet to collect and exchange data. |
| Intrusion detection system (IDS) | A device or software application that monitors a network or systems for malicious activity or policy violations. |
| Intrusion prevention system (IPS) | A system that is used to detect and prevent identified threats. |
| ISO/IEC 27001 | An international standard on how to manage information security, and details the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). |
| Keylogging | The use of a program or device to record every keystroke made by a user, especially to gain fraudulent access to passwords and other confidential information. |

| Term | Definition |
|---|---|
| Layered security (defence in depth) | A security approach that uses multiple measures to protect computer systems and sensitive data. |
| Least privilege principle | A security concept in which a user is given the minimum levels of access necessary to complete their job functions. |
| Malware, computer virus | Software designed specifically to damage or disrupt systems, such as viruses and ransomware. |
| Managed detection and response (MDR) | A service that combines technology and skills to remediate and respond to threats and cyber risk. Usually offered to organisations by specialist service providers. |
| Managed security service provider (MSSP) | A security supplier that provides an organisation with some information security management capabilities, which can include monitoring, management of intrusion detection systems and firewalls, overseeing patch management and upgrades, and responding to security incidents. |
| Man-in-the-middle (MitM) attack | A security breach where the attacker secretly intercepts and relays the communication between two parties. |
| Multi-factor authentication (MFA) | An authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. |
| Need to know principle | A security principle that restricts access to information to individuals who need the information to perform their job duties. |
| One-time authorisation code (OTAC) | A token (code) that is valid for only one login session or transaction, preventing the risk of access from potential intruders. |
| Online scam, digital fraud | Criminal activity using the Internet for deceptive or fraudulent purposes. |
| Online tracking | The practice by which websites and other online services collect and share information about user activity. |
| Operating system (OS) | Software that manages all of the other application programs on a computer. |
| Password | A secret word or phrase used to gain access to a particular system or secure information. |
| Password manager | An application that is used to store and manage the passwords that a user has for various online accounts and security features. |
| Password strength assessment | The evaluation of a password to determine its strength, typically based on length, complexity and unpredictability. |
| Patch | A piece of software designed to update, fix or improve a system, application or its supporting data. Often includes fixes of security vulnerabilities. |

| Term | Definition |
|---|---|
| Patch management | The process and practice of acquiring, testing, and installing patches (code changes, updates) to an administered system. An important aspect of maintaining security. |
| Penetration testing | An authorised simulated cyberattack on an application, system, or network, performed to evaluate the security of the target. |
| People, Process, Technology (PPT) | A concept that underscores the interdependence between the human, procedural and technical aspects of an organisation. |
| Personal data | Information related to an identified or identifiable individual. It includes, but is not limited to, names, addresses, phone numbers, email addresses and identification numbers. Also referred to as personal information or personally identifiable information (PII). |
| Personal identification number (PIN) | A (numerical) code used in electronic transactions, a form of simple authentication. |
| Phishing | A type of online scam where attackers impersonate trustworthy entities to deceive targets into revealing sensitive information, such as passwords, credit card numbers or other personal or organisational details. |
| Privacy | The right of individuals to keep their personal data confidential and control who has access to it. See also: General Data Protection Regulation (GDPR). |
| Privilege management | The process of assigning and revoking privileges or access rights to systems and data, typically related to user roles within an organisation. |
| Protective measure | Any action, device, procedure, technique or other control designed to safeguard users and assets against a threat. |
| Ransomware | Malware that blocks access to a system or data (files on a storage) until a sum of money is paid. Typically deployed by cybercrime actors. |
| Risk | The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. |
| Risk management | The practice of identifying, analysing, and mitigating or accepting the risks faced by an organisation. |
| Role-based access control (RBAC) | An access control mechanism defined around roles and privileges, regulating who can access what within an organisation. |
| Secure coding | The practice of writing programs that are resistant to attacks by malicious actors. |
| Secure communication channel | A communication pathway that is secured through encryption to prevent unauthorised access to the transmitted data. |

| Term | Definition |
|---|---|
| Secure development lifecycle (SDL) | A process followed for a software development project, in which the development team prioritises security and follows secure coding practices. |
| Secure file sharing | Tools utilising cryptographic mechanisms to share files securely, protecting them from unauthorised access and disclosure. |
| Security architecture | A detailed framework that documents an organisation's security controls and protective measures. |
| Security assessment | The review of an organisation's information systems by evaluating how well they conform to a set of security criteria. |
| Security awareness training | A program or ongoing campaign that educates employees about the risks associated with poor information security practices and trains them to practise cyber hygiene and digital self-defence. |
| Security baseline | A set of basic security objectives which must be met by any given service or system. |
| Security certification, attestation, assurance | Demonstrable measures taken by an organisation to show compliance with established security frameworks and security standards. |
| Security champion | An advocate for security awareness within a team or function of the organisation. |
| Security compliance | Adherence to laws, regulations and standards governing information security, data protection and privacy. |
| Security compromise | The result of a security incident where the security of a system or data has been exposed, leading to data breach or data loss. |
| Security control | Safeguards or protective measures designed to avoid, detect, counteract or minimise security risks to people, data and systems. |
| Security event | An occurrence in a system or network indicating a possible breach of security policy or failure of security controls, that may be relevant to security. |
| Security framework | A set of guidelines or best practices used to manage information security and address cyber risk. |
| Security incident | An event that actually or potentially undermines the confidentiality, integrity or availability of information or a system. |
| Security information and event management (SIEM) | Solutions that provide real-time analysis of security alerts generated by hardware and applications. |
| Security intelligence | Information relevant to defending an organisation against malware, data breaches and advanced persistent threats. |
| Security Operations Centre (SOC) | A centralised unit in an organisation responsible for monitoring security events, assessing and defending against security incidents. |

| Term | Definition |
|---|---|
| Security policy | A set of guidelines and procedures designed to protect information from being damaged, lost or accessed by unauthorised individuals. |
| Security posture | An organisation's overall information security strength and its ability to react to security incidents and to maintain cyber resilience. |
| Security standard | A set of criteria that provide a baseline for measuring security. |
| Social engineering | Manipulating people into revealing confidential information; a type of attack in which someone impersonates a trustworthy entity, or exploits weaknesses in human psychology in some other way. |
| Software as a service (SaaS) | A software licensing and delivery model in which software is provided on a subscription basis and is centrally hosted. |
| Spam | Unwanted or unsolicited messages sent over the Internet, typically to a large numbers of users, usually for the purposes of advertising, phishing or spreading malware. |
| Supply chain attack | A cyberattack that seeks to damage an organisation by targeting less secure elements (for example a vendor) in their supply network. |
| System and Organization Controls 2 (SOC 2) | A framework for managing and securing data. |
| Tactics, techniques, and procedures (TTP) | The behaviour and operational methods of adversaries and threat actors. |
| Technical and organisational measures (TOMs) | Security measures that are put in place to protect data and information, including both technological solutions and appropriate organisational policies. |
| Threat | A potential cause of an unwanted incident, which may result in harm to a system or organisation. |
| Threat actor | A person or entity that is responsible for a security event or security incident that impacts, or has the potential to impact, the safety or security of an entity's assets. |
| Threat modelling | A process by which potential threats can be identified, enumerated and prioritised from a hypothetical threat actor's point of view. |
| Token | A type of code, often used in multi-factor authentication, e.g. a one-time authorisation code sent to a mobile device. |
| Transport layer security (TLS) | A protocol that creates a secure communication channel between applications and users on the Internet (replaced secure sockets layer, SSL). |
| Two-factor authentication (2FA) | A version of multi-factor authentication. |
| Username, user ID | A unique string of characters that identifies the user to a system, usually as part of the user's credentials. |

| Term | Definition |
|---|---|
| Virtual private network (VPN) | A private network that is built over a public infrastructure, allowing users to exchange data over a secure and encrypted connection; for example to protect private web traffic from snooping, interference and censorship. |
| Vulnerability | A weakness in a system or its design that could be exploited by a threat. |

## Government organisations responsible for information security and cyber risk guidance

- Austria: Secure Information Technology Center (A-SIT, "Zentrum für sichere Informationstechnologie" in German)
- European Union: The European Union Agency for Cybersecurity (ENISA)
- Finland: Finnish Transport and Communications Agency (Traficom)
- France: National Agency for the Security of Information Systems (ANSSI, "Agence nationale de la sécurité des systèmes d'information" in French)
- Germany: Federal Office for Information Security (BSI, "Bundesamt für Sicherheit in der Informationstechnik" in German)
- Hungary: National Cyber Defence Institute (NKI, "Nemzeti Kibervédelmi Intézet" in Hungarian)
- Netherlands: National Cyber Security Centre (NCSC-NL)
- Norway: Norwegian National Security Authority (NSM)
- Sweden: Swedish Civil Contingencies Agency (MSB)
- United Kingdom: National Cyber Security Centre (NCSC)

## Projects and references by privacy and security advocacy groups

- Security-in-a-Box – digital security tools and tactics, a project by Front Line Defenders: https://securityinabox.org/
- European Digital Rights (EDRi), an association of civil and human rights organisations from across Europe: https://edri.org/
- The Data Detox Kit, a project by Tactical Tech: https://datadetoxkit.org/
- CryptoParty – a decentralised movement present in most European countries: https://www.cryptoparty.in/

# Template: statement on information security

## Introduction

[*Organisation's name*] is committed to maintaining the security and privacy of its [*staff, clients, partners, donors, etc.*]. Security is protection from, or resilience against, potential harm. Privacy is the right to be left alone, and freedom from intrusion – in compliance with the EU's General Data Protection Regulation (GDPR). All staff [*and contractors]* are expected to meet the requirements stated in this document.

## Cyber hygiene: a baseline of mandatory requirements

Cyber hygiene is a set of habits practised continuously to maintain the healthiest possible security posture. The goal of cyber hygiene is to keep sensitive data secure and to protect it from theft or compromise. Privacy and data protection also depend on the same security measures.

- Online discretion: be careful with what information you share.
- Establish and cultivate an awareness of phishing, business email compromise (BEC) attacks and other forms of social engineering.
- Separate work and individual data/ devices to stop data sprawl.
- Avoid installing new software, accessing a new service online or subscribing to a new tool or solution – check beforehand with your supervisor or IT.
- Protect your accounts and digital identities: use a unique, strong password and multi-factor authentication (MFA) for all your apps and online accounts.
- Protect your devices: install software updates and security patches on devices for the operating system and for applications. Turn on automatic updates.
- Protect your network access: do not use public or open wireless connection (wifi). Choose known networks that are secured – make sure the wifi needs a password.

## Report suspicious activities

Poor cyber hygiene can lead to security incidents and data breaches. Maintaining security and privacy depends on all of us. If you find something, say something: [please send questions and report concerns to [*email address/ instant messaging contact; e.g. "security@example.com"*].

## Standards and frameworks

Security standards and frameworks are structured approaches to managing information security and protecting against cyber risk. For smaller organisations, knowing about them is relevant when selecting partners or vendors, purchasing software, or procuring new technology solutions. A higher level of trust can be given to companies that have a security certification or publish a security attestation report.

| Standard/framework | Relevance |
|---|---|
| ISO/IEC 27001 | An international standard on the implementation of an Information Security Management System (ISMS). Compliance shows that a business has a holistic approach to information security. |
| NIST Cybersecurity Framework (CSF) | Developed by the U.S. National Institute of Standards and Technology (NIST), this framework provides guidelines on managing and reducing cyber risk. It is scalable and can be applied to organisations to improve resilience against security threats, independent of their size and sector. |
| System and Organization Controls 2 (SOC 2) | Also referred to as "service organisation controls", this certification developed by the American Institute of Certified Public Accountants (AICPA) shows that service providers (cloud providers, data centres, IT managed services) manage the data of their clients and customers in a secure manner. It evaluates controls pertinent to security, availability, processing integrity, confidentiality and privacy. |
| CIS Critical Security Controls | Developed by the Center for Internet Security (CIS), these controls offer a prioritised approach to information security, outlining key actions for defence. Less comprehensive than ISO/IEC 27001 or NIST CSF but a good system specific starting point for organisations with limited resources and know-how. |
| Payment Card Industry Data Security Standard (PCI DSS) | For businesses that handle credit card transactions, PCI DSS compliance is essential. It offers guidelines on securing and strengthening payment card transaction systems. |
| EU General Data Protection Regulation (GDPR) | With an extraterritorial reach, GDPR compliance is mandatory for all organisations dealing with EU citizens ("data subjects"). It focuses on data protection and imposes strict rules on data collection, storage and processing. |
| Cloud Security Alliance (CSA) Guidelines | For organisations that heavily rely on cloud services, CSA provides technical guidelines for ensuring cloud computing security. The CSA also maintains the Security Trust Assurance and Risk (STAR) Program, which encompasses key principles of transparency, rigorous auditing, and harmonisation of standards for cloud vendors. |

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

***Publisher***
Civil Liberties Union for Europe e.V
Ebertstraße 2,
10117 Berlin,
Germany

***Website:***
liberties.eu

***Contact info:***
info@liberties.eu

***The Civil Liberties Union for Europe e. V.***
Ebertstraße 2,
10117 Berlin,
Germany

***Subscribe to our newsletter***
https://www.liberties.eu/en/subscribe

***Reference link to study***
Please, when referring to this study, use the following web address:
https://www.liberties.eu/f/hfgng1

***Photo credit***
Luke Stackpoole/Unsplash.com

***Follow us***