Cyber Risk

What is a cyber risk?

The term cyber risk brings together all the risks and dangers linked to the use of digital technologies that are likely to compromise the confidentiality, integrity, authenticity and availability of data and production tools.

No company is immune, whatever its size, nature of activity or sector (whether commerce, services, health, finance or industry). It only takes one incident to jeopardise a company's entire operations.

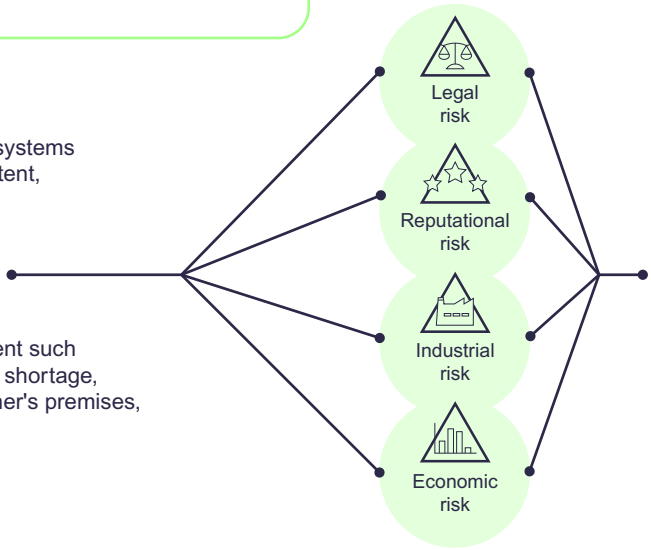
Be vigilant: make the right decisions and apply best practices.

Dangers linked to cyber risks

When the security of data, however sensitive, is compromised, these cyber risks can have serious consequences: financial losses, interruptions to trade, business disruptions, security risks, production stoppage or reputational damage.

Internal risks
Negligence, misuse of computer systems or data, human error, malicious intent, lack of training, etc.

External risks
Cyberattacks, infrastructure incident such as water damage and fire, energy shortage, component shortage, fire on partner's premises, changes to regulations, etc.



Preventing and reducing risks
There are several ways of reducing cyber risks: implementing security policies, employee training, establishing emergency andrecovery procedures.

« In our interconnected world, cyber threats are an unavoidable reality. It is imperative to take all necessary measures to protect your company and employees. »

Dimitri Konstantas, Professor and Director of the Information Science Institute at the University of Geneva

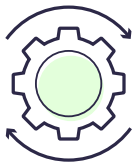
This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0
All the contents of this document may be shared, copied, reproduced, distributed, communicated, reused and adapted by any means and in any format, provided that the author is mentioned (State of Geneva) and the same license is used for all related content (CC – BY – SA 4.0).

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX
h e g Haute école de gestion Genève
UNIVERSITÉ DE GENÈVE

Learn more

The essentials

Protect your files and devices

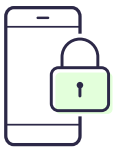


Keep your software and systems up to date by applying automatic updates to your applications, web browsers, operating systems, devices and equipment.

Lock access to devices (computers, tablets, smartphones, etc.) with a strong password created either by yourself or a password management service, and do not leave devices unattended in public places. Use caution when using public Wi-Fi networks.

Set up multi-factor authentication to access your corporate network (for SMS, email, authentication application, etc.).

Back up important files offline, on an external hard drive or on the cloud so that you can access them even if your equipment is lost, broken or stolen. Be sure to store your paper records just as securely.



Use an encryption key to protect sensitive, critical information on your company devices, such as laptops, tablets, smartphones, removable hard drives and USB drives, and cloud storage solutions.

Use software and/or protection systems such as an antivirus, firewall, and intrusion detection and prevention systems (IDS/IPS).

The security of your business is paramount!
Call in support from specialists.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

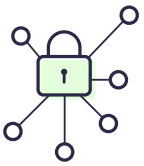
The essentials

Protect your network

Enable your firewall to control and filter network traffic by allowing or blocking certain types of communication and content based on predefined rules.

Secure your router by changing the default name and password and turning off remote management. Remember to change the password regularly.

Make sure your wireless network offers WPA2 or WPA3 encryption and is enabled to protect information passing through your network from unauthorised persons.



Define restrictive lists of devices that are allowed to access the corporate network.

Rename your Wi-Fi network from its default so that you cannot be identified by it. For even more discretion, you can hide the network.

Make security part of your company culture

Create a culture of security by regularly training your teams and informing them of new risks and vulnerabilities.

Implement a business continuity plan (BCP). Your BCP should describe how to back up your data and keep your business running in the event of an incident, attack, or damage. Put this plan in writing, communicate it to everyone involved with your company, and test it on a regular basis.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Preparing a strategy

How can businesses reduce cyber risk?

Regardless of size, all companies should be implementing the following **5 steps**.

1 Identify

- Make a list of all the equipment, applications and services used by your business. This includes computers, smartphones, and tablets, but also peripheral devices such as printers, as well as any other objects or machines connected to your network or the internet.
- Create and share a company cyber security policy that covers:
  - The roles, responsibilities and access of each employee, as well as any third party – person or company – who could access sensitive information.
  - What to do to protect yourself against attacks and limit any damage.

2 Protect

- Monitor who has access to your company network and who can use your computers and other devices (employees, customers, partners, service providers).
- Use and configure security software to protect your data.
- Encrypt sensitive data and keep encryption keys in a secure, separate location.
- Define a regular, automated backup plan for your data (see pages 15-16).
- Update all your software regularly or set up automatic updates.
- Regularly train everyone using your equipment. Help your employees understand the issues and risks for themselves and the company.

3 Detect

- Set up active monitoring for your equipment to detect unauthorised access by people, devices (like USB drives), and software.
- Monitor unauthorised connections to your network.
- Investigate any suspicious activity on your network and systems.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Preparing a strategy

4 Respond

Write a **business continuity plan (BCP)** so that, in case of a service interruption and/or attack, you can:

- Identify and contain the attack.
- Report the attack to the relevant authorities.
- Warn your customers, teams and partners whose data may have been exposed.
- Ensure that your business activity continues.
- Address vulnerabilities and restore activity.
- Update your cyber risk management policy.
- Anticipate possible unforeseen scenarios (such as a natural incident) that could damage your data.

Test and update your BCP regularly

5 Restore

After an attack:

- Identify, list and analyse the damage caused (such as damaged equipment, data leak, compromised access, etc.).
- Secure and decontaminate your work environment and the affected equipment.
- Repair and restore equipment and parts of your network that have been damaged.
- Keep your teams, customers and partners informed of progress during the restoration process.

To help you set up and implement a protection strategy against cyber risk, call on support from a specialist company.

Did you know?

In the event of a cyberattack, the average time it takes for businesses to get back to full operations 22 days..

To find out more, visit the national **Federal Office for Cybersecurity (OFCS)** website.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Physical security of digital assets

Cyber risk prevention starts with physical security

Weaknesses in physical security can expose sensitive data.

For example:

- An unsecured computer or mobile phone left on a train.
- Old documents disposed of at a waste collection point accessible to everyone.
- Files and computer equipment stolen in a burglary.

Digital corporate responsibility

Raising employee awareness of digital responsibility is essential, because people are often the most vulnerable link when it comes to cyber threats, and employees' actions can have a direct impact on the company's security and reputation.

Read our guide on digital corporate responsibility

How to protect your equipment and physical records

- Securely store your paper files and electronic equipment containing sensitive information in a closed, fire-resistant cabinet or room (use specialist companies).
- Limit access to archives, files and equipment to authorised persons and keep a record of all access.
- Securely destroy obsolete files and data. Use a document shredder or hire a company specialising in secure destruction to dispose of paper documents and data carriers; don't just throw them away or recycle them.
- Regularly remind your teams to lock their workstations when they are away and not leave sensitive documents, USB keys, hard drives, mobile phones etc. unattended.
- Ask your teams to secure smartphones according to current best practices if they are being used for work.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Physical security of digital assets

How to secure access to your devices

The loss, theft or misuse of a device can have serious consequences.

Secure the data contained on these devices by following best practice:

- Use strong passwords: A strong password is long (12 characters minimum), complex and unique (containing special characters such as !?@#%, upper and lower case letters and numbers).
- Make sure these passwords are generated and stored securely using a password manager.
- Set a different password for each account or application.
- Differentiate between private and business passwords.
- Never share your passwords.
- Change your passwords regularly.
- Lock devices with codes.
- Set up multi-factor authentication (MFA) to access your corporate network and various tools (e.g. one-time password and/or double authentication).
- Turn off Bluetooth on your devices when you don't need it.
- Limit connection attempts to a maximum of 5 to protect from intrusions.
- Encrypt mobile devices containing sensitive information. Also encrypt internal or external exchanges that contain sensitive information.
- Store your encryption keys in a secure location that is separate from the company infrastructure.
- Before selling on or donating old computers, mobile devices, printers or other electronic equipment, use data destruction software or hire a specialist company;
- don't just erase the data.
- Regularly inform your teams about cyber risks and train them, providing them with the appropriate equipment and continued learning opportunities.
- Encourage the good security practices both in the office and at home.
- Share your **business continuity plan (BCP)**. Each team member should know who to contact and what steps to take in the event that equipment or records are lost or stolen.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Securing remote access

Your teams and partners should follow high security standards when accessing your network remotely, whether they are using your company equipment or personal equipment.

Protecting equipment during remote access

- Secure your router: systematically change the default name and password settings, and keep software up to date.
- Encrypt data sent over networks or on devices that connect to your network remotely by default.
- Configure the settings on smartphones, tablets and laptops: change the default settings to prevent automatic connections to wireless networks.
- Keep anti-virus software up to date and schedule automatic updates on all equipment that may connect to your network remotely (including computers and mobile devices).

Working remotely

When you are off company premises, follow company rules regarding the use of IT and security tools. Make sure you are applying good cyber security practices at home and on the go.

Providing teams and partners with tools that maintain high security levels

- Make sure that any access from external locations goes through a router that implements the best wireless network encryption standards (such as WPA2 or WPA3).
- Use a corporate VPN to give your teams remote access to your network, encrypting traffic between devices and the internet.
- Set up multi-factor authentication (MFA) and the use of strong passwords.
- Make sure the Wi-Fi network for guests is separate from the company network and provide guests with unique passwords.
- Include security clauses in all contracts with partners needing to connect to the company network.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Web hosting

Are you looking to create or update your website?

If you do not have the necessary skills to set up a website, call on a specialist in web design and hosting. There are many web hosting options available depending on your needs. When comparing services, security should be a central concern.

Questions to ask your future provider

- ☐ Is the site secured by a TLS protocol, and is it included in the hosting contract?
- ☐ I would like to use my domain name for my professional email addresses. Can you set up a security mechanism, such as SPF, DKIM or DMARC?
- ☐ Who is responsible for security updates an site maintenance, and how often are these carried out?
- ☐ Once my website is live, who will have administrative and editing rights?
- ☐ Will multi-factor authentication be implemented for people with administration and editing rights to the website?

Secure your website with TLS

TLS is a security protocol designed to provide secure communications over a computer network. It is used to encrypt data shared over the network, ensuring the confidentiality and integrity of information exchanged between two systems. When TLS has been properly implemented on your website, your URL will start with “https://”.

Authenticate your e-mail addresses

You can configure your company’s email addresses to use your site’s domain name (for example: mybusiness.ch / name@mybusiness.ch). To ensure that scammers cannot send emails in your name by stealing your organisation’s domain name, you must authenticate e-mails. To do this, you can used verification mechanisms or standards like Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, and Reporting & Conformance (DMARC).

Maintain your website

From the outset, you need to clarify who is responsible for maintaining your website. This may be an internal role or carried out by an external service provider, depending on the skills you have. Ensure that website and security components are regularly updated.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Insurance and legal aspects

Managing a cyber incident and getting your business back up and running is costly and complex.

Cyber insurance offers for SMEs in Switzerland can include technical assistance, protection against financial losses, public liability cover and legal aid. Taking out insurance does not relieve you of responsibility, nor does it protect you against cyber incidents.

Checklist for taking out cyber insurance

- ☐ Is the site secured by a TLS protocol, and is it included in the hosting contract?
- ☐ Conduct a study of your company's activities to create an inventory of the greatest risks depending on the level of impact.
- ☐ Determine how much coverage your business needs.
- ☐ Evaluate the different insurance options and choose the one that best meets your business needs based on its activities.
- ☐ Check the details of each policy's coverage and exclusions.
- ☐ Learn about the risks covered by the insurance, including data loss, personal information claims, data breaches, and legal and professional fees incurred by third-party breaches.
- ☐ Ensure that your insurance policy covers the risks to which the company could be exposed and that the compensation matches the level of risk insured.

To help with your risk assessment, check the **Digital Platform Observatory.**

Legal framework

In Switzerland, cyber risk management falls within the legal framework governed by the Information Security Act (LSI) and Data Protection Act (LPD).

Regulatory frameworks vary by region and type of business activity. It is essential to find out about the regulations in effect in the countries where the company is active to ensure compliance with the applicable laws.

For more information, see **the Global Data Protection Regulations guide**.

Did you know?

According to Article 19 of the Federal Data Protection Act (LPD), you are obliged to inform individuals when you collect data about them.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Phishing

How does it work?

You receive an email or text message

It appears to come from a person or company you know, asking you to respond by email or by clicking on a link to provide details about your identity, password, or other sensitive information about the company.

It looks authentic

It's easy to fake logos and create fake email addresses. Typically, scammers use familiar business names or pretend to be people you know.

It's urgent

The sender urges you to act quickly or urgently, suggesting that negative consequences will occur if you do not act.

What happens next

If you click on a link, hackers can identify that you have interacted with the message and continue soliciting you with the aim of extracting information or tricking you into taking action, such as paying money.

If you receive a message that seems suspicious to you

- **Check the sender's e-mail address**
- **Check URLs by hovering over them before clicking on them**
- **Do not respond to the message**
- **Never reveal your identity**
- **Never provide bank details**
- **Never pay money**
- **Do not open attachments**

Report fraudulent messages to the Federal Office for Cybersecurity (OFCS): https://www.ncsc.admin.ch/

Report it!

If you have received a phishing email or discovered a phishing site, report it at **https://antiphishing.ch**

Test your teams!

Carry out internal tests regularly to assess your employees' awareness and understanding of cyber risks and issues for the company, for example through a false phishing campaign.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Case study

It only takes one click...

When someone clicks on a fraudulent link that installs ransomware, the entire company network shuts down and data is held hostage. Hackers demand a ransom in the form of a bank transfer or cryptocurrency to unlock access to the data.

In the meantime, all the company's activity is blocked. The data needed for the business to operate, including sensitive information about customers, teams and commercial activities, end up in the hands of hackers.

Nearly 80% of cyber incidents result from human error within the company or from partners.

The Federal Office for Cybersecurity (OFCS) recommends filing a criminal complaint in all cases. To do this, contact the cantonal police. You can find your nearest police station on the **Switzerland e-Police** website.

How do computer viruses work?

There are several ways that malware can get installed in a system:

- Through fraudulent e-mails with links or attachments that put your data and network at risk. These phishing e-mails (see previous page) are behind most ransomware attacks.
- Visting infected websites, scanning a QR code, or clicking on links that automatically download malware to your computer or smartphone.
- Connecting a device or computer which is external to the company on your network or computers (USB key, hard drive, smartphone, etc.).
- Running unverified or untrusted applications.
- Authorising external links to be opened or macros launched when accessing documents sent to you by someone outside the organisation.

What to do in the event of a ransomware attack?

The **OFCS** advises against paying a ransom, as there is no guarantee that your data will be returned to you. Additionally, giving in to blackmail helps finance criminal activities and encourages criminals to continue their activities or start again.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Preventing attacks and their consequences

Write a business continuity plan (BCP)

A BCP will enable you to keep your business running in the event of a cyberattack or cyber incident. Put the plan in writing, share it internally, and test it on a regular basis.

Raise your teams' awareness of social engineering

Train and inform your teams on the different manipulation techniques used to encourage a person to share information, however sensitive. The data may be personal or confidential information allowing access to an organisation's computer network. Techniques consist of exploiting the human factor, for example by usurping the identity or role of a person or organisation.

Before you click on a questionable link…

- Check the domain name really exists and that it matches the site you want to visit.
- Check that the site is secure: the URL should start with "https" (the "s" indicating that the information is encrypted), and check that the certificate has not expired or become invalid (the padlock next to the URL should not be crossed out).
- Make sure you're talking to a real, trustworthy person or organisation, and that you're not about to download malware or share access with a scammer.
- If in doubt, talk to people around you. This will help you determine whether the request is real or a phishing attempt.
- If in doubt, call the supplier directly or the person who supposedly sent you the email. Be wary of the number in the message and instead consult your contact list.

Be proactive!

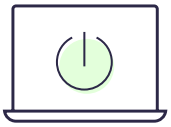
Did you know?

In the event of a cyberattack, the average time it takes for businesses to get back to full operations 22 days.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

What to do in the event of an attack

1 Limit the damage



- Cut off the internal (Wi-Fi and LAN) and external (WAN / internet) networks.
- Identify the infected computer or devices and turn them off. If you cannot identify them quickly, carry out these processes on all your IT stock.
- Change all passwords.
- Perform a check on all devices (computers and servers), or have them checked, to ensure that they are not infected.

2 Raise the alarm

- Follow company procedures to notify your manager or IT service provider.
- Alert your colleagues and share your experience when phishing occurs, as these attempts often involve more than one person in a company.

3 Report it

- If any data or personal information has been compromised, notify those affected.
- Report fraudulent messages to the **Federal Office for Cybersecurity (OFCS)**.
- Report any violations to the police.

4 Communicate

- Keep your employees, partners, clients and customers informed.

Refer to the federal law on information security (LSI)
L'article Article 74b lists the authorities and organisations subject to the obligation of reporting a cyberattack. This concerns many companies in different sectors.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Example of a data backup strategy

A backup consists of duplicating the information needed for the proper functioning of the company on an external medium and/or space, and keeping it secure so that it can be accessed in the event of a cyber incident. Without a backup, it is impossible to restore company data.

Setting up a backup plan

1

Map the data

- Take an inventory of all your data.
- Assess how critical this data is to the business.
- Organise and categorise the data.
- Define the location of the data: identify the devices that use it and the locations where it is stored.
- List the people and systems with access to this data.

2

Prioritise the data

Organise your data by level of importance. To do this, ask yourself the following questions:

- What files and information are essential to the overall functioning of the organisation and each of its services or departments? (For example: accounting, contacts, customer files, diaries, HR, strategic and commercial documents, etc.).
- What data and documents are essential and non-recoverable in the event of loss, theft or destruction of equipment?

3

Decide on backup locations

For a good backup strategy and rapid recovery of company data, back up your data in 3 different locations:

- **Storage on a backup solution within the organisation (e.g. backup server)**
- **Offline storage on a hard drive held within the organisation in an easily accessible place (e.g. secure room)**
- **Storage on a disk stored outside the organisation (e.g. bank safe)**

For greater security and autonomy, you can perform an additional backup on a NAS drive (mini file server), SAN (a backup solution suitable for medium and large businesses), the cloud, or a data centre.

If storing on the cloud, be sure to find out where the servers hosting the data are kept, the company's legal obligations for data hosting, and the laws that apply depending on the country. A cloud solution that stores and processes data on national territory is recommended.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Example of a data backup strategy

4

Put in place a backup schedule

It is important to back up company data regularly. The frequency can be determined based on your organisation's activities.

For example, you might set up a daily backup, supplemented by weekly and monthly backups. Regularly monitor and test backup archives and recovery processes.

The schedule will allow you to restore your data easily and quickly in the event of an incident, with minimal to no loss.

5

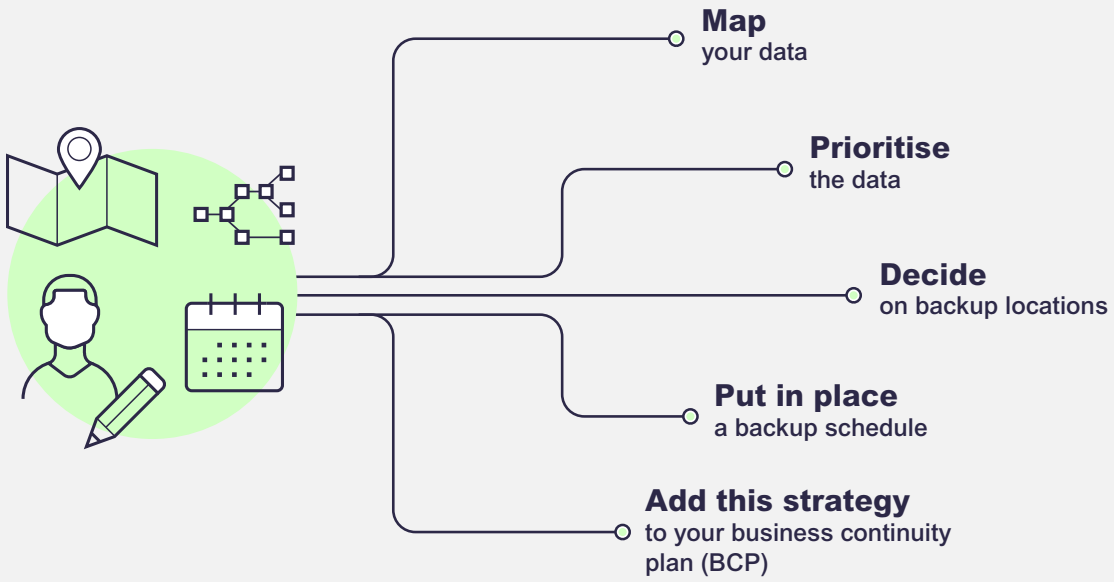
Make this strategy part of your business continuity plan (BCP)

The BCP describes how to maintain business continuity to minimise interruptions and operational disruptions (see page 5).

Among other areas, it defines the procedure to be followed for securing and restoring data in the event of a computer incident.

A backup strategy is an essential part of this procedure, as it determines how your IT can be recovered to start up activities again.

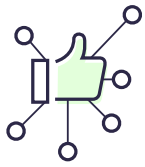
Backup plan



This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

In summary

Bad practices



- Believing that cyber security is only an IT issue.
- Adopting new technology and new digital practices without first analysing the risks and opportunities.
- Underestimating the impact risk or likelihood of a cyber incident.
- Neglecting the importance of a continuity plan and data backup strategy.
- Collecting and processing more information than necessary..

Best practices to protect your equipment, network and data

- Keep your software up to date.
- Secure your wifi router with WPA2 or WPA3 encryption.
- Back up your data on a regular basis.
- Require strong, unique passwords for all equipment and access.
- Enable multi-factor authentication.

Best practices to protect your staff, business, customers and partners

- Draw up a policy where access to resources is restricted by default and only permitted by relevant individuals.
- Limit the information published on your company site. Avoid any information that identifies people and their role in the company to prevent identity theft or social engineering.
- Train your teams by providing them with appropriate equipment, as well as internal or external continued learning opportunities.

The security of your business is paramount!
Call on support from specialists.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0