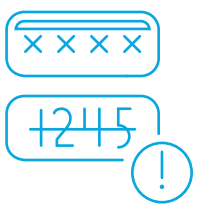
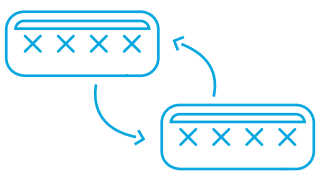
# What can businesses do to fortify their controls

## Managing employee risk

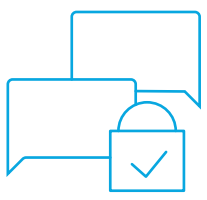
Employee awareness and promoting cybersecurity best practice and train staff to recognise suspicious emails




Maintain strong passwords, and enforce strict rules where possible



Ensure passwords are regularly changed, for example every 3–6 months

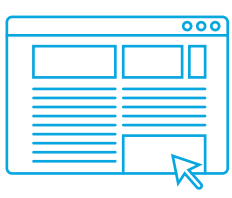


Communications to employees, customers and media

## Managing IT security

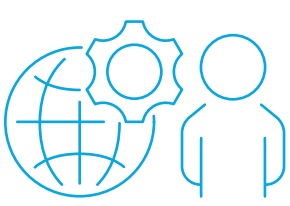
Activate firewalls on all computers and devices connected to the internet

Use a reputable anti-virus service and ensure it automatically updates on a regular basis



Monitor your network and investigate suspicious behaviour scan and filter emails before delivery to employees

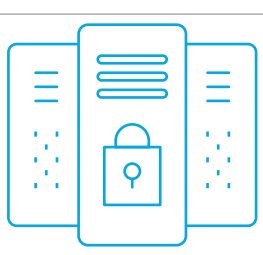
Apply software patches to keep systems up to date



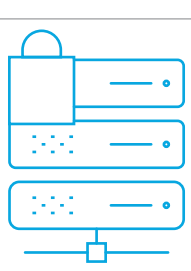
Segment your network

System users should be required to identify and authenticate themselves with usernames and passwords

Activate two-factor authentication for hosted services

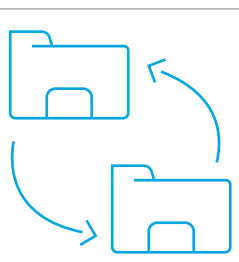


Ensure only administrators are granted full administrative access to computers/systems



Prevent low-level users from using unnecessary system functions and data. Reserve those rights for privileged administrative accounts

Regularly update the software on all systems

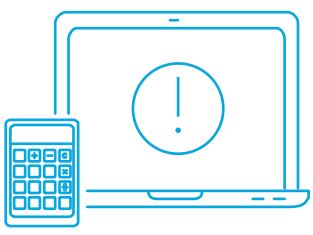


Regularly backup important data to a separate location. It might be necessary to restore your system if your data is deleted or modified without authorisation. Having a backup copy is crucial for the recovery process

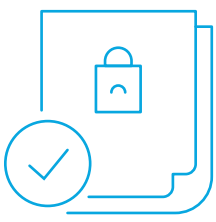
Having a process of attack and threat prevention, detection and containment

## Managing operational risk

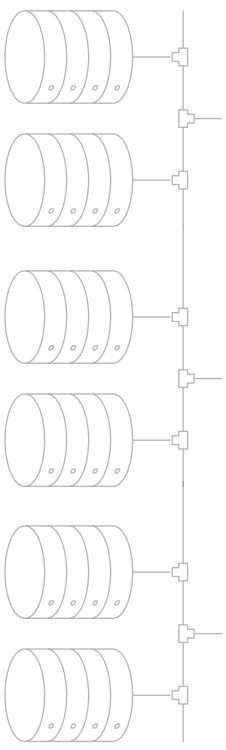
Remove unused user accounts (previous staff members, for example)



Make IT-budgets (cyber security) one of the main topics for business

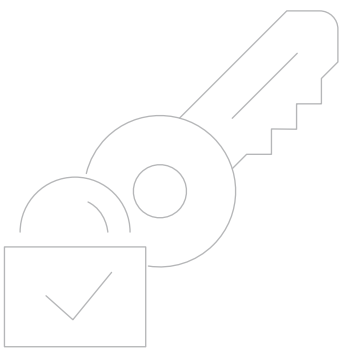


Ensure IT and cybersecurity controls, policies and protocols are in place



Familiarise senior management with IT security

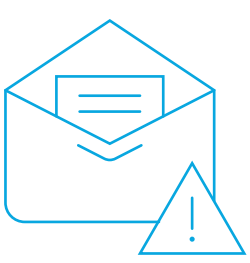
Work with experts and train cyber-incident scenarios



## Managing cybersecurity incidents and crisis planning

Have a crisis incident plan in place and test it upfront

Have a crisis escalation protocol in place to the board, the authorities, data protection authorities



Have a crisis communication plan with scenarios in place for brand and reputation management