Cyber security incident response plan template

Even the most well-established businesses face threats such as data leaks and security breaches. Minimising the operational risk of cyber security incidents comes down to preparation, early detection and implementing strategies to reduce the impact.

Preparation and prevention

- [ ] conduct training to educate employees on cyber security best practices and how to identify potential threats
- [ ] identify the risks to these assets and what steps you need to take to minimise the impact to your business
- [ ] execute incident response plan in a test scenario on a regular basis
- [ ] generate plan on how to operate if a system is down
- [ ] identify the financial assets, data and technology that are most critical to your business operations and maintain a current asset inventory including software
- [ ] delegate roles and responsibilities for identifying and handling cyber security incidents
- [ ] implement regular backups and test restore data
- [ ] organisation security policies created and communicated to the business

Incident detection

Develop a process for detecting and reviewing unusual activity, and conduct regular testing to identify weak spots in your network.

Signs can include:

- being unable to access accounts
- changed passwords
- moved or missing data
- malfunctioning software or hardware
- people receiving spam emails from you
- excessive pop-up ads or website redirects
- dwindling storage space
- newly created users
- changes to user permissions
- monitoring log files

Enter your process here:

Incident reporting

When a suspicious event occurs, document the type and severity of the incident, notify relevant team members and assess potential impacts.

This includes:

- [ ] documenting the nature of the incident
- [ ] when it occurred
- [ ] where it occurred
- [ ] the cause of the incident
- [ ] who has been impacted so far
- [ ] who needs to be notified
- [ ] preserve evidence

Enter your process here:

Incident response

Contain the security threat as soon as possible by isolating the affected systems. This can involve disconnecting from the network, shutting down the affected device server and securing crucial business data and information.

Enter your process here:

Recovery process

Once the threat is contained, it's time to reboot your servers and return to business as usual. Here it's important to also detail the steps your employees need to take to restore their systems safely.

Enter your process here:

Note: If customer data has been compromised, make sure to inform the affected parties and inform them on the steps taken to rectify the situation.

Review and optimise

- [ ] assess your IT security and improve systems and processes to prevent future incidents
- [ ] evaluate the incident and identify lessons for the future
- [ ] update your cyber security management plan to incorporate learnings from the incident