

10 STEPS TO REDUCE the impact of cyberattacks

Learn how you can position your organization to discourage cyberattacks and respond decisively to an attack if one occurs.

1 Back it up

Back up your systems regularly and securely and keep an offline copy. Test your backup restore process.

2 Have a plan

Your organization must have an incident response plan (IRP) in place and run through it with various cyber playbooks.

3 Get cyber insurance

Some policies may require a certain level of organizational cybermaturity, and most can help handle the costs associated with a cybersecurity incident.

4 Gather a team

Have a team ready to assist when needed, including people from internal/external IT, HR, legal, and cybersecurity/incident response teams, as well as other key stakeholders.

5 Test your environment

A vulnerability assessment/penetration test of your environment can help determine any gaps to be filled. Tests should be conducted twice a year or during technology changes.

PROACTIVE

Don't wait to be a victim of a cyberattack before taking steps to secure and protect your data.

6 Implement your IRP

A well-crafted and well-rehearsed IRP can save you time when dealing with a cyber incident.

7 Submit a claim

Call your cyber insurance provider for advice and next steps in making a claim. RSM has relationships with many of the top insurance providers and understands what is needed for a cyber insurance claim.

REACTIVE

You've fallen victim to a cyberattack and are not sure of the next steps.

8 Make it privileged

Breach counsel can help determine what constitutes PII, PHI, PCI or other protected/regulated data, and when notification is required. Retaining breach counsel also protects your communication under lawyer-client and litigation privilege.

9 Get the right help

Recovering too quickly from a breach may lead to a lack of forensic evidence needed for a claim. RSM can help you gather what is required for an investigation, while assisting in the timely recovery of your systems.

10 Compile lessons learned

Once the breach has been contained and investigated, RSM can work with you to determine lessons learned and additional steps to mitigate future cyberattacks.

RSM's dedicated team of cyber professionals can help you take the appropriate steps to resist cyberattacks, and are there for you if you ever do fall victim to one. If you have a question about any of the 10 steps above, please reach out. We are here to help.