corsica technologies

How to Prevent and Recover from a Data Breach

Even the most well-protected organizations can experience a data breach. When it comes to recovery, how you prepare for a potential breach determines how it affects your organization. Use these tips to put your business in a better position in the event that a data breach occurs.

How to Prevent a Data Breach

Here are some steps to take prior to a breach to help mitigate its effects:

1. **Establish business continuity and data recovery plans**. Make sure you regularly rehearse them.
2. **Identify and document essential systems and recovery priorities.**
3. **Regularly back-up your systems.** Ensure that the backups are tested on a regular basis.
4. **Regularly update and patch your systems.**
5. **Enable and enforce multi-factor authentication.** This should be enabled and enforced for all logins.
6. **Implement the principle of least privilege.** This should be applied across the entire organization.
7. **Configure firewalls.** Set them up to deny any traffic that is not required and explicitly allowed.
8. **Require ongoing cybersecurity awareness training for all employees.** Employees must be trained on the importance of cybersecurity and the practices that will keep both their information and that of the organization safe. They should be able to identify malicious emails or activities and be aware of incident reporting procedures.

How to Prevent and Recover From a Data Breach

corsica technologies

Recovering from a Data Breach

Here are some steps to take if a breach has occurred:

1. **Contain the breach.** Immediately isolate impacted systems to limit spread across the organization. Terminate any external access that is not critical to business operations or essential to recovery.
2. **Assemble your crisis management team.** Determine the extent of the breach, cyber insurance options, public relations announcements to both the media and employees, any legal or regulatory requirements, and any required forensics.
3. **Gather and preserve evidence.** Post-incident forensics require system and network logs, bitwise copies of impacted systems and memory snapshots. This evidence will help guide the investigation, build out events related to the cyber kill-chain and may also be required for any insurance or legal proceedings.
4. **Remediate and restore systems.** In an orderly and methodical manner based on your organizations priorities, ensure infected systems are not reintroduced to any remediated networks.

Ready to take cybersecurity to the next level?

Our team of cybersecurity experts is ready to help. When you partner with Corsica Technologies, you get a team of highly certified and experienced IT experts and cybersecurity engineers that support your unique business needs and challenges 24x7x365.

REQUEST A CONSULTATION