Digital Security
Progress. Protected.

CYBER**RESILIENCE**

IDENTIFY + PLAN

Achieving cyber resilience: ESET’s four-step approach to business continuity.

Step 1: Identify and plan

Technology is so fully integrated into our lives and businesses, we tend to take it for granted. That’s a mistake when it comes to cyber resilience.

Your path to true cyber resilience starts with reviewing your current situation. Here are examples of the questions you should ask yourself.

- **Think about the systems you access every day, and how you access them. Consider things like payroll, accounts payable, HR files, client lists, etc. What would happen if one or more of them became inaccessible? How quickly could you replace or replicate the data that they hold, or the functions they perform?**
- **Look beyond the production systems themselves and consider how they are accessed. What would happen if a key employee’s password was compromised, giving an intruder access rights?**
- **If you had to take your directory, remote access controllers, or other central network administration systems down for remediation, how could you operate in the interim?**
- **If you lost a critical system, could you get by with a manual process, short-term? How quickly could you spin up a new server instance and recover the data and functionality from a backup?**

It’s this type of long-view consideration of contingencies, business continuity plans and recoverability that separates cyber resilience from what most people think of when they hear the word cybersecurity.

Resources

Need some guidance on taking the first step toward cyber resilience?

An expert from the ESET partner network of managed service providers can assist you in developing a business continuity plan to support your efforts.

Contact your authorized ESET reseller for details.

Checklist: Taking a proactive look ahead

- Incorporate your third-party supply chain and the part you play in others’ supply chains in your planning; upstream and downstream business that rely on each other require complementary cyber-resiliency capabilities.
- Upgrade any legacy systems that rely on outdated technology and can’t be patched against security threats. If you can’t update them, then segment them from the rest of your systems.
- Regularly refresh your continuity plans to account for operational changes. Understand how the business can operate while under cyberattack when access to systems may be limited.
- Conduct a practice crisis scenario, and make sure everybody knows their roles and what is expected of them.
- Keep a crisis emergency contact list and update it regularly.
- Consider outsourcing and contracting with a managed services provider if you lack the resources to deal with a major incident. Keep in mind that waiting until an incident happens to mount a reactive response is not an effective cyber-resiliency plan.
- Include a data backup and recovery solution in your continuity plan so you can replace any data lost during a cyberattack or natural disaster.
- Test backups and disaster recovery systems to ensure your ability to recover not just the data, but to restore the ability to operate the business.