Digital Security
Progress. Protected.

# CYBERRESILIENCE  RECOVER

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

# Step 4: Recover

Too often, backup and recovery are treated as "in case we need it" activities. Businesses dutifully run backups, but give little consideration to whether the systems being backed up can be fully recovered. Result? Backups that can't restore the systems impacted back to their full functionality.

**Remember:** The goal of a cyber resilience strategy is to keep the business running through an attack and recovering to a semblance of normal operations as quickly as possible. Therefore, anticipating how you will effectively recover from a cyber incident is an integral part of your initial planning.

Of course, having a good backup that you can recover from is absolutely critical if a ransomware attack manages to encrypt your systems and data. But consider this as well: When there's an intrusion on your network, an attempt to intrude, or the suspicion of one, reaction time is critical.

Once an intruder has compromised one or more devices on your network, the next step is to move laterally through the system, use compromised accounts to gain access to other systems, escalate privileges and gain administrative access.

Responding to an active, in-progress intrusion may involve shutting down production systems or isolating them to limit any further damage to the business. If you suspect that a key system has been badly compromised, your best strategy could well be to restore from a backup.

Anticipate these possible scenarios as part of your business continuity planning, and it will pay huge dividends when you're faced with an attack. You'll have to spend fewer hours analyzing the situation and formulating the best response, at a time when minutes and seconds count.

## ESET Solutions

**ESET's partner Xopero provides** total protection, backup and recovery of your business data onsite or in the cloud. Utilizing advanced cloud backup for computers, servers and virtual environments, it allows you to easily create backups, and synchronize and restore data from servers and workstations.

## Checklist: Plan ahead to restore lost data

- Evaluate which data is critical. Which data and documents are so essential that the business can't run without them? What kind of data losses would be devastating? How quickly do you need to restore access to them?
- Think outside your network. You should be able to instantly recover entire operating systems, virtual machines and data in cloud-based applications.
- Consider and plan for email recovery. Emails between team members and with partners, clients and customers may contain valuable information that isn't replicated elsewhere. If you use email as a filing cabinet, make sure you can recover it if necessary.
- Establish your two critical metrics for backup and recovery. Recovery Time Objective (RTO) states how long applications can be down without causing significant damage; Recovery Point Objective (RPO) establishes how much of your most-recent data can be lost before your business is dramatically harmed.
- Combine cloud and local solutions. Apply the 3-2-1 rule: have three copies in two different internal locations and at least one outside the company. Make more frequent backups to the local storage, but be able to restore from outside the company as well; the most convenient external location is the cloud.
- Use dedicated backup software. Backups done with manual methods are performed less often, and often turn out to not include everything you need to properly recover. An automated system makes recovery faster, too.
- Make sure the backups are secure. Ransomware gangs encrypt your backups if they can get to them. Local backups should be completely disconnected from the network if at all possible. If you use a cloud-based backup provider, ask how the backups are protected.

20220512