eset Digital Security
Progress. Protected.

CYBER**RESILIENCE**

Achieving cyber resilience: A four-step approach to business continuity

The term "cybersecurity" typically refers to efforts to defend computers and networks against successful attacks and infiltration.

Cyber resilience goes several steps further—acknowledging that attacks may succeed; focusing on the ability to continue operations during and after an incident; and applying learnings to build back even stronger.

While it's designed to improve your response to cyberattacks, the strategy can also help you weather other business disruptors—including power outages, employee errors and natural disasters.

Building resilience into your organization helps you anticipate, recognize and respond to attacks, greatly enhancing your overall security posture.

Cyber resilience isn't a "one and done" process. Ideally, it is a cycle to be reviewed and improved upon regularly.

Use ESET's guide to develop your plan, based on these four steps:

- **Identify and plan**
- **Protect**
- **Detect and respond**
- **Recover**