AXONIUS

Common myths about cyber resilience

Security teams are tasked with cyber resilience projects, but often find themselves in a series of conflicting articles and ambiguous terms on the topic.

While not a complete guide, this document aims to address common misconceptions about cyber resilience:

MYTH 1

Cybersecurity and Cyber Resilience are the same

While related, cybersecurity and cyber resilience are distinct concepts. Cybersecurity focuses on preventing attacks, while cyber resilience encompasses the ability to withstand, adapt to, and recover from cyber disruptions for a full cybersecurity program.

MYTH 2

Advanced technology alone ensures Cyber Resilience

Investing in advanced technology is important, but it's not sufficient on its own. Cyber resilience requires a comprehensive approach that includes people, processes, and technology. Examples of that include having an effective communication strategy, and collaborating with stakeholders in charge of BCP and Crisis Communications.

MYTH 3

Cyber Resilience is the same as Organizational Resilience

Organizational resilience is an enterprise initiative that includes cyber resilience and other resilience components to ensure the business is better prepared for different types of disruption beyond digital threats to the organization.

Resilience component	Typical organizational role
Resilience Program, Framework, Metrics	CRO; COO; CFO; Resilience Leader
Cyber Resilience	CISO; BCM Leader
Supply Chain Resilience	Supply Chain Leader; Procurement
IT Resilience	CIO
Cloud Resilience	CIO
Data Resilience	CIO
Infrastructure Resilience	CIO
Operational Resilience	CRO; COO; Resilience Leader; BCM Leader; CISO
Workforce Resilience	HR Leader

Source: Gartner

MYTH 4

Small businesses don't need to worry about Cyber Resilience

Small businesses are often targeted by cybercriminals precisely because they may have weaker security measures. Every business, regardless of size, must prioritize cyber resilience.

MYTH 5

Once secured, always secured

Cyber resilience is an ongoing process that requires continuous updates, monitoring, and improvement. The attack surface changes regularly, threats evolve constantly, and the definition of critical systems change as the business adopts technologies, requiring a regular reassessment of security measures.

MYTH 6

Manual processes are a reliable fallback

Many organizations believe they can rely on manual processes if their systems are compromised. However, in today's digital economy and with the growth of both IT and OT, manual processes are often too limited or cumbersome to sustain operations for extended periods.

MYTH 7

Existing disaster recovery plans are sufficient

Traditional disaster recovery plans may not be adequate for cyber attacks, as they typically focus on geographically limited incidents rather than adversarial threats. Disaster Recovery scoping (systems and recovery time/point objectives) are static by nature and may not take into consideration all assets compromised by an attacker.