The Logical Advantage

TeamLogicIT®
Your Technology Advisor

JUNE 2024

4 Cornerstones of Cyber Resilience

According to PwC's latest Global Crisis and Resilience Survey, nine out of 10 company leaders polled reported their organizations had experienced a business disruption during the past two years. In this same study, three quarters of executives also said these disruptions had "medium to high impact" on operations.

No wonder these same leaders listed "resilience" among their top strategic priorities going forward.

In the broadest sense, business resilience is an organization's ability to anticipate, endure and recover from crises, such as economic downturns, operational breakdowns and other types of catastrophic failure. In the physical world, these catastrophes can be caused by multiple factors beyond a company's control, such as natural disasters. In the cyber realm, the most common culprit is cybercrime; which makes the key to cyber resilience cybersecurity.

What are the foundational elements of cyber resilient cybersecurity? Here are four cornerstones:

- **Assess to Protect** – Understand your technology perimeter. Identify any security gaps. for any business looking to develop cyber resilience. Implement preventative measures.
- **Respond to Recover** – Plan to recover from disaster before an emergency strikes. Streamline policies, processes and practices for speed and efficiency amidst crises.
- **Design for Flexibility** – Anticipate adapting tactics and solving problems at full speed.
- **Train for Learning** – Regular drills and ongoing education facilitate the continual refinements and continuous improvement necessary for high cyber resiliency.

We have deep expertise in core technological disciplines supporting cyber resilience, such as cloud computing, collaboration tools and backup and disaster recovery routines (BUDR.) Give us a call.

The Logical Advantage

Viewpoint

5 Building Blocks of Cyber Resilience

The rising tide of ransomware attacks set records last year despite efforts by law enforcement agencies around the world. Researchers monitoring this cybercrime favorite have detected increases in malicious activities from 2022 to 2023 as high as 50%.

According to the Cybersecurity and Infrastructure Agency (CISA) one hack alone last year compromised more than 3000 U.S.-based organizations and another 8000 globally.

But the news isn't all disturbing. During the last 12 months, there have been signs of progress in the fight against cyber extortion. Studies show that a growing number of ransomware victims are refusing to pay. One research team found that in Q4-2023 the proportion of afflicted firms agreeing to pay ransoms dropped 29% to a record low.

Why? Analysts believe these are the reasons:

1. Increasing cybersecurity awareness and education, such as threat notifications.
2. Refined and rehearsed incident response plans.
3. Persistent security diligence, such as incursion monitoring.
4. Consistent backup and disaster recovery (BUDR) processes and practices.
5. Sharpening the focus of remediation efforts on root causes and vulnerabilities, such as human error.

Taken together, these measures deepen and fortify cyber resilience, a company's ability to anticipate disruptions from catastrophes like ransomware, improve at avoiding them over time, optimize operational response in the event of breaches and then recover at maximum speed.

IT Strategy

MSPs Help Remove Resilience Roadblocks

Seven out of 10 executives responding to last year's PwC Global Crisis and Resilience Survey reported a lack of confidence in their organization's ability to respond sufficiently to business disruptions. Researchers blamed this assurance lag on studies showing too few companies have the "foundational elements of resilience" to feel successful. In cybersecurity terms, this means many firms have lost faith in their ability to:

- Anticipate threats
- Deflect most attacks
- Respond rapidly to incursions
- Refine policies and processes afterward
- Translate learnings into improvements later

How can business leaders restore confidence in these resilient practices? By removing some obstacles in their way.

Here are common resilience roadblocks, where a managed services provider's (MSP) support can help shove them aside:

- **Shadow IT** is when team members procure and use technology without your IT department's knowledge and permission. Your MSP can help by conducting an asset inventory as an external help desk, rather than as an internal auditor.
- **Scarce Funding** for cybersecurity is typical in the absence of operational information. Your MSP can help by gathering metrics about thwarting threats that demonstrate return on IT investments.
- **Shaky Culture** around cybersecurity grows without regular awareness campaigns. Your MSP can help by supporting education programs with outside specialists.

Give us a call to learn more.

Visit our blog for more trending technology articles at TeamLogicIT.com/blog.

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor