C&W Business

Securing beyond resilience

As the digital economy continues to grow at pace, the need to protect your network has never been greater. Cyberattacks increased by a whopping 125% between 2021 and 2022, and this continued in 2023 as well, according to the World Economic Forum's Global Cybersecurity Outlook report.[1]

Be it ransomware, hacking, or malware, businesses need to put robust and resilient cybersecurity systems in place to prevent downtime or business disruptions due to cyberattacks.

Typically, IT security professionals use a preventive strategy to address the growing risk of cyberattacks. This follows the principle of building robust systems that are able to fight cyberthreats before they cause any damage to the systems.

The traditional cybersecurity strategy of deploying systems to prevent a cyberattack seems to have limited success as the danger of cyberthreats increases worldwide. Further, it is becoming tougher to prevent a cyberattack as the digital ecosystem continues to grow, and the increasing popularity of remote working and Bring Your Own Device (BYOD) means that enterprises have to rethink traditional cybersecurity strategies.

Growing relevance of the antifragile approach

In this context, there is a growing acceptance of a fundamentally different approach to "antifragility". Introduced by Nassim Nicholas Taleb in his book "Antifragile:[2] Things That Gain From Disorder" in 2021, the concept is essentially used to describe objects that benefit from experiencing some form of failure or stress. "Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better," explains Taleb in his book.

Taleb describes three states of fragility, resilience, and antifragility in his book. While fragility is destroyed by chaos or disorder, resilience remains unaffected, and anti-fragility actually benefits from disorder.

The antifragility concept essentially reverses the conventional cybersecurity approach, which sees any potential attack as an enemy. Instead, the antifragile concept sees cyberattacks as unavoidable. It doesn't work to prevent a cyberattack but instead treats a possible attack as something that will strengthen the system. This perspective is confirmed by the fact that 93% of oranisations experienced an intrusion in 2022 alone, according to Fortinet's State of Operational Technology and Cybersecurity Report.[3]

Focusing on response as well as prevention

What this means is that the antifragile approach accepts the futility of preventing an attack and acknowledges that a cyberattack is not just inevitable but is, in fact, a learning opportunity. The antifragile way of thinking is particularly relevant in these current times, in which the conventional prevention-only approach is turning out to be ineffective against increasingly frequent cyberattacks.

[1] World Economic Forum - Global Cybersecurity Outlook 2023

[2] Nassim Nicholas Taleb - Antifragile

[3] Fortinet's State of Operational Technology and Cybersecurity Report

While firewalls, anti-virus software, and internal controls and processes are key aspects What this means is that the antifragile approach accepts the futility of preventing an attack and acknowledges that a cyberattack is not just inevitable but is, in fact, a learning opportunity. The antifragile way of thinking is particularly relevant in these current times, in which the conventional prevention-only approach is turning out to be ineffective against increasingly frequent cyberattacks. While firewalls, anti-virus software, and internal controls and processes are key aspects of your security posture, they are just part of a wider successful strategy for responding to the deluge of cyberattacks. Your business still needs to be prepared for a scenario in which the protection and detection stages are not enough to hold off an intrusion. In such a situation, a rapid response and recovery makes all the difference.

Organisations need to prepare for this inevitable reality to minimise the damage and use the attack to improve cyberresiliency. To move from a solely preventive cybersecurity strategy to an antifragile way of doing things calls for a fundamental shift in mindset.

In this context, organisations need to use a combination of the traditional preventive cybersecurity approach and build cyberresilience. This would enable them to not just quickly bounce back in the event of a cyberattack but use it as an opportunity to improve the system's robustness. While the conventional cybersecurity strategy helps prevent incidents, cyber resilience will enable the organisation to not just return to the pre-incident state in case of a security incident but also incorporate the learnings from the incident to withstand similar attacks in the future. The antifragile way of building resilience is centred around continuously learning and improving from cyberincidents. As incidents of cyberattacks continue to grow, it is time to reimagine cybersecurity strategies to bring them more in tune with the changing reality. The antifragile approach is helping organisations do just that!

C&W Business can help organisations build cybersecurity systems that focus on putting up a robust and resilient response to cyberattacks. With our comprehensive solutions portfolio, businesses can prepare for and respond to any issues that arise, feeling confident in the knowledge that their systems are protected, and their strategies are continuously evolving to meet the changing threat landscape.

At **C&W Business,** we're your catalyst for transformative success.
From Cybersecurity to Cloud, Data Centres, Unified Communications, and Connectivity, our streamlined solutions ensure scalability and security. With the Pan-Caribbean region's largest and most reliable network.