IN FOCUS

CIO priorities: Business continuity, resilience and mitigating risk

Is your organisation prepared for the hybrid workforce of the future?

Companies stand at a crossroads in the wake of the COVID-19 pandemic. They have rushed to support remote workers with makeshift infrastructures that tested their information security skills. Now, these environments are becoming more permanent as new hybrid working practices persist.

While pressures are mounting to reopen offices and reinvigorate city centres, as many as 82 percent of company leaders plan to let their employees work remotely at least part time, according to Gartner, Inc. For many companies, the office will never look the same again. PwC's Remote Working Survey found fewer than one in five executives expecting a complete return to pre-pandemic conditions.

Remote working, at least some of the time, will be a permanent fixture. But with the new remote paradigm comes new challenges, especially in security.

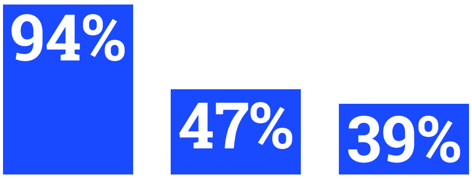
As businesses reconcile themselves with these long-term changes, they are accepting the need for a renewed focus on both security and business resilience. The Logicalis Global CIO Survey found that the pandemic has made business continuity and resilience more important to 72 percent of organisations. Over half of all respondents also said that the pandemic taught them the need to adopt disaster recovery plans, and 80 percent said that they had spent more time increasing their security defences over the last 12 months. As companies evolve, they must maintain and improve this security and resilience as they strike out with new innovations in areas such as customer and employee experience. No matter the technology, without the right security policies and procedures in place an attack can take place. The key is making sure the entire business is educated on security risk and management to support new security technologies.

Securing the digital workplace of the future

Creating a cohesive digital workplace ecosystem for this new workforce, regardless of physical location, involves more effort and strategy than simply handing out laptops, turning to cloud apps, and using a VPN (Virtual Private Network).

A secure remote-work strategy is essential for business resilience with increasing threats of cyberattacks on remote workforces. Exacerbated by the pandemic, there are now 648 cyber threats per minute, according to a recent security intelligence report. 2020 saw unprecedented attacks as cybercriminals exploited vulnerabilities in businesses' security perimeters due to the shift to remote working.

Cybersecurity leaders must consider the expectations of the next normal when it comes to assessing both current cybersecurity activities and long-term cyber-risk strategies. This leads to some important questions. *How can organisations manage data securely regardless of whether it is located at home, inside your organisation or with their suppliers? And how should businesses implement effective and seamless security controls to all the devices, both corporate and personal, used by their employees?*



LOGICALIS' SURVEY RESULTS REVEAL HIGH AWARENESS OF BUSINESS RISK, WITH 94 PERCENT OF RESPONDENTS ACKNOWLEDGING SOME FORM OF SERIOUS THREAT OVER THE NEXT 12 MONTHS. CIOS CITE DATA BREACHES (47 PERCENT) AND MALWARE AND RANSOMWARE (39 PERCENT) AS THE BIGGEST RISKS TO THEIR ORGANISATIONS.

Businesses urgently need to adopt additional security measures

Despite CIOs being aware of the increased risk, awareness didn't translate uniformly into action. Risk mitigation wasn't a common performance metric among organisations. Barely a third of them cited risk mitigation as a measure of performance. Moreover, while most CIOs cite business continuity and resilience as a key takeaway from the pandemic, only 27 percent of organisations listed business continuity and resilience as a top three priority during the next 12 months, putting it second-to-last in the rankings.

Where businesses have invested in mitigating security risks, the lion's share (66 percent) have put money into technology such as firewalls, cyber protection software, and password management. Half of all companies invested in more staff training.

Although CIOs recognise the importance of implementing disaster recovery plans, fewer than half (45 percent) of businesses have done so. Only 40 percent have implemented business continuity plans that would help their companies keep running during major disruptive events. Investing in tools alone won't protect organisations; they must have policies and playbooks at the ready to support their operations through disruptive times.

Technology is only as efficient as you make it

Protecting themselves from disruption and security threats isn't the only focus for modern businesses recovering from the pandemic. They also see the need to explore new opportunities through innovation, adapting their existing business model to new conditions, and potentially even grabbing new market share by investing in new products and services.

79%

79 PERCENT OF CIOS CONSIDER INNOVATION A FOCAL AREA OVER THE NEXT 12 MONTHS AS THEY STRIVE TO INCREASE EMPLOYEE AND CUSTOMER EXPERIENCES.

One area where companies are investing in new technologies and innovation is the internet of things (IoT). Logicalis found 96 percent of CIOs are using this technology in some form. The most popular use case is improving customer experience, with 55 percent of respondents focused on it. Increasing operational efficiencies (52 percent) and enhancing existing products and services (46 percent) come close behind.

The key focuses and priorities for CIOs and their businesses over the next 12 months are monumental tasks and often aren't easy to achieve. 73 percent of security and IT executives' express concerns about the continued vulnerabilities of any hybrid working model.

Businesses can't afford to risk their security. Data breaches and operational disruptions can lead to financial, legal, and regulatory ramifications. Yet at the same time they must invest in innovation, using new technologies to keep themselves at the forefront, enhance customer service, and generate more revenues.

The best of both worlds, increased innovation and enhanced security

While innovation and risk mitigation seem to be opposing forces, businesses see a clear link between the two, with customers wanting to deal with companies that are secure and care for their data. Businesses that have suffered a major data loss often see a larger percentage of their customers move to competitors as a result. The survey found 95 percent of respondents using innovation to create business resilience, indicating that these two forces can be complementary in an organisation.

For example, well-planned cloud migrations can simultaneously boost security and introduce powerful new capabilities that streamline product and service development. They can support collaboration and innovation among distributed workforces with maximum efficiency.

The cloud helps companies create flexible business continuity frameworks. It offers a holistic approach to security that can anticipate and detect emergent threats before they attack an operation's infrastructure, protecting hybrid workforces.

Toby Alcock, CTO of Logicalis says: "Over the last 18 months, many businesses set up interim solutions to cope with remote working, with security and disaster recovery very much experiencing a trial by fire. Some measures worked, but more action is needed to secure hybrid workers and enhance business resilience for the long-term."

"Businesses should adopt a holistic security approach with the capabilities to anticipate and detect threats before they even take place. Investing in optimising security operations that give a complete view will allow organisations to mitigate risk and adapt to future obstacles, whether cyberattack-related or further market disruption. With a comprehensive plan, created with advice from third-party experts, companies can rest assured knowing they're protected."

Planning for both innovation and risk means constructing a foundation for change that is agile, flexible, and secure. Many companies lack the in-house skills to engineer an effective foundation that addresses strategic, tactical, and operational realms mapped to a business's overarching objectives. Therefore, companies are investing in third-party support to help. The survey revealed that 35 percent of companies had invested in more third-party expertise, and that 31 percent of CIOs saw supporting business continuity as a driver for using external services.

A partner can provide holistic services throughout the lifecycle, to ensure your business reaches its full potential as it grows. With the right strategic approach, companies can combine security, resilience, and innovation, to create a clear competitive advantage. Working in partnership with a third-party expert, organisations can remove the barriers to innovation, drive business growth and unlock future success in the rapidly emerging digital economy.

To learn more about how our services can help your organisation please get in touch at: info@logicalis.com