DXC TECHNOLOGY

# Building cyber resilience in a remote future

August 2021

# Building cyber resilience in a remote future

## By Anandh Maistry, Director and Regional Head Cyber Security APAC

As the dust settles on the rapid disruption and digitisation driven by the pandemic, organisations across APAC are shifting from a crisis mindset to now planning strategically for the future. According to a recent **Harvard Business Review report,** sponsored by DXC Technology, during the pandemic, 86 percent of organisations increased their employees' ability to work remotely. While at the time it was unknown whether this would be a permanent shift, it's safe to say that in a post-pandemic era, employees will continue to work from anywhere, on the device of their choice, and have access to a plethora of collaboration tools.

While this allows businesses to be agile and adapt to change, it also results in massive amounts of data being created across the organisation, as well as more entry points set up than ever before. This, combined with the increase in cyber threats such as extortion-based ransomware, phishing, and business email compromise, has created new challenges for security teams and shone a light on the need to be resilient.

What does it mean for an organisation to be cyber resilient in an era of constant change? When it comes to security, businesses that are set up for success are the ones that not only understand what their environment looks like, but also have clear visibility over the attack surface. They have a solid disaster recovery plan in place, allowing them to bounce back quickly and suffer minimal disruption to productivity if they are breached. To bolster cyber resilience organisations should focus on three key areas:

80%

of organisations have expanded the collection and use of data across their organisation

34%

say they assess risk and build in new security measures every time they undertake initiatives to do this

## Remove the complexity

There's no denying that CISOs and their security teams are under constant pressure to protect all people, process, and technology from cyber risk. This is often a daunting task, especially in a remote environment. In fact, almost half (49 percent) of those surveyed by Harvard Business Review and DXC said they were highly concerned about the increased IT network expansion and complexity as a result of remote working.

It might sound simple, but one of the most important steps an organisation should take to overcome complexity, and move forward on the path to resilience, is to simplify their approach to security. This can be achieved across three stages. Firstly, ensuring the organisation is compliant in the way it operates, meeting all its regulatory requirements. Then, it's integral to understand how vulnerable the organisation is to cyber threats by observing the external environment and identifying all possible entry points. Finally, it is critical to have a plan in place for if (and when) the organisation is breached. This includes a robust disaster

A Zero Trust model, forces the implementation of stronger authentication and verification processes. It also drives greater visibility over data, with a holistic view on how data is being captured, why it's being retained, how it's being used, where it resides, and who has access to it.

recovery strategy as well as considerations for how to manage any associated reputational and operational damage.

Additionally, threats such as ransomware continue to rise, organisations need to have the foundation of security hygiene in place. Getting the fundamentals right is a key component to achieving resilience. This includes following best practice guidelines such as the **Essential 8** provided by the Australian Signals Directorate (ASD), or the Notice 655 issued by the Monetary Authority of Singapore.

## Protect data, first and foremost

As organisations across APAC continue to enable their employees to work remotely, security teams must move away from an old way of operating that focused on securing a traditional network infrastructure. They instead must shift their attention to think about how to protect the data itself, rather than the associated network segments.

While 80 percent of organisations have expanded the collection and use of data across their organisation, only 34 percent say they assess risk and build in new security measures every time they undertake initiatives to do this. This shows a clear disconnect between the data flowing through the organisation and how protected it is.

To combat this, organisations should implement a Zero Trust approach that treats every user and piece of data as a threat, whether it sits inside or outside the organisation. A Zero Trust model, forces the implementation of stronger authentication and verification processes. It also drives greater visibility over data, with a holistic view on how data is being captured, why it's being retained, how it's being used, where it resides, and who has access to it. Knowing this information first and foremost is paramount to being able to then put appropriate controls around the data, which will minimise the risk of data theft.

## Security at the centre

Cybersecurity continues to be a key business imperative – so much so that boards are asking for regular updates around the organisation's security posture and resilience. Despite this, security continues to be an afterthought for many businesses, driven by a false sense of assurance that they are in a robust enough position to absorb any risk or reputational damage should they suffer a breach.

Rather than treating security as an afterthought, organisations must take a 'secure by design' approach, where they build protection into every new technology and process they implement. While only 34 percent of organisations deem artificial intelligence (AI) and machine learning (ML) to be very important to their security operations, these technologies can be key drivers for building resilience through prediction and prevention. This is because they make it easier to analyse vast and complex data sets and detect potential threats quickly, freeing up security teams to focus on other pressing tasks.

This security-first mindset should be embedded into the culture of the organisation, with a focus on protecting employees by educating them. As employees continue to engage and collaborate remotely, it's critical they understand the importance of securing their data and personal information. Beyond having the critical hygiene checks in place such as multi-factor authentication and regular password updates, organisations should also look to provide regular security updates to their employees. As employees are the first line of defence for an organisation and cybercriminals often target them by relying on human error to gain access to sensitive information, businesses should additionally run awareness campaigns to ensure security is front of mind and employees are cognizant of their actions online.

In the post-pandemic era where employees continue to work remotely and cybercriminals continue to target the attack surface, it's up to organisations to prioritise resilience. This should be done by taking a straightforward, methodical approach to understanding the cyber environment, implementing Zero Trust models to protect data, and building a culture of security that touches all people, process and technology in the organisation.

Insights from Harvard Business Review and DXC Technology can be found in the following report: **Cybersecurity in the Era of Intelligence and an Expanding Attack Surface.**

Learn more at
**dxc.com/security**