Disruption and security: what we've learnt in 2020

By Anandh Maistry, Director & GM Digital Security ANZ

DXC.technology

The disruption faced by businesses in 2020 has revealed both the effectiveness of their operations and areas in need of improvement, highlighting the importance of elements such as business continuity, cloud technologies to enable remote operations, and cybersecurity. **DXC's Beyond Disruption 2020 Business Pulse,** which looked at shifts in local business leaders' perspectives on technology during this tumultuous time, found that 66 percent of organisations identified security as one of the top 5 most important tech investments in the next 12 months.

The research reiterates that cybersecurity is no new kid on the block. The introduction of local and global data protection regulations and a string of high-profile breaches over the past few years have proved why it is and should be a primary business imperative – and the recent pressure on businesses to quickly transform is another reminder of this. It's no surprise that **90 percent** of Australian organisations plan to lean on enhanced security measures to carry them into the future.

The speed and scale at which organisations have needed to accelerate digital transformation efforts is something no one was prepared for. It showed that every organisation has work to do when it comes to its security posture – even the ones that looked prepared from the outside.

To be able to improve in the future, it's important for businesses to reflect on the past few months as they plan for the next few. Although we're still navigating our way through this new normal, here is what we've learnt so far:

Lesson 1: Hygiene matters in the digital world

When it comes to being cyber safe, businesses that have even the most basic level of cybersecurity hygiene – following the **Essential 8** as provided by the Australian Signals Directorate (ASD) and **Top 10** from Cert NZ – will be propelled forward in terms of preparedness. Making sure their environment is patched, knowing who has access and doing advanced diagnostic assessments on anything that gets released are all crucial rungs on the hygiene ladder. While this won't make organisations fully immune from threats, it will reduce their level of vulnerability.

Australian and New Zealand organisations have looked to new technologies to aid the drastic shift to remote working and new ways of engaging with their customers. DXC found that 34 percent have invested in mobile applications to engage with customers and staff, 22 percent in remote learning platforms and 22 percent on virtual staff such as chatbots and digital assistants. Organisations should approach these technologies with the same security hygiene and processes as they would any other implementation.

It's also important for them to take a step back – rather than getting caught up in the rush to digitise – and have a look at the detail design and interconnections with other solutions, to be able to make better decisions and drive efficiencies where possible.

Lesson 2: Embrace a culture of cybersecurity

The unexpected turn of events in 2020 has also reminded us that protocols and governance can be put in place to mitigate risk, but when it comes to human nature, there is always the possibility that rules will be overlooked – deliberately or not.

Civilians have been trusted to wash their hands regularly and stay home when feeling unwell, and businesses too have put their trust in employees to keep sensitive information protected and establish strong security protocols in their home environments.

We've seen a massive increase in the number of organisations allowing most of their staff to work from home – from 7 percent before the crisis, to a staggering 44 percent now – and cybercriminals have quickly started to take advantage of this. If a cybercriminal gains access to an employee's credentials, they can get to their data and do anything online that the employee can. All it takes is one employee clicking on a phishing link or saving an important document to a vulnerable personal device to unravel years of hard work from security teams.

This is why building and sustaining a culture of security is paramount, so employees remain aware of evolving threats and learn how to avoid them. This culture should be driven from the top, with C-level executives and managers reiterating cybersecurity fundamentals in a simple way so that it's easy for employees to understand them.

They could host regular 'lunch and learns' that cover company-wide, client and personal security, interactive training sessions that test employee knowledge on how to spot a phishing scam, or primers that ensure employees' home routers are as secure as they can be. As organisations have more of these conversations, security starts to cascade through the business and becomes embedded in its DNA.

Lesson 3: Businesses are only as safe as their weakest link

Organisations do not operate in silos, and businesses are at risk of exposing others in their supply chain if they themselves are compromised. This reminder that we are all in this together has shone a light on the importance of supply chain security, open communication and increased collaboration. Creating best security practices in all these areas, and upholding them across all corners of the business, is critical, as one weak link could easily create a chain reaction.

82 percent of organisations DXC surveyed have rethought their business strategies around technology to manage disruption. As many continue to find their feet and maintain policies around fraud prevention and using onshore alternatives for currently offshored IT services, there is opportunity to share knowledge and learnings to become stronger and move forward together – as one secure unit.

Looking forward

2020 has shown us that no one is immune when it comes to cybersecurity. Breaches can spread like wildfire, leaving organisations and individuals vulnerable – especially as many enterprises have had to move out of their comfort zones and away from legacy operations and technology. We don't yet know the full impact of the changes experienced and the decisions made when it comes to cybersecurity, implementing new employee processes and adopting new technologies. But it's evident that the industry has an even more heightened awareness that security should be at the forefront of business operations.

For organisations to thrive in the long-term, they need to seize the opportunity to increase their level of preparedness, while continuing to get the basics right. Honouring protocols, respecting the process and working with partners and peers will help them move in the right direction.

CP_1559a-21. August 2020