PROACTIVE PROTECTION

Martin Riley *reveals why it's vital to put security at the forefront of digital transformation*

It's no secret that COVID-19 has had a huge impact on digital transformation. Many companies have been forced to accelerate their transformation efforts and have invested more in new technologies over the past year than they may have the previous five. And the desire for transformation isn't set to slow down any time soon – it is expected that 65 percent of the globe's GDP will be digitalised by 2022, with the digital transformation market forecasted to grow to $3,294-billion by 2025.

It doesn't come as a surprise that businesses from all sectors and of all sizes are embracing innovation and going digital. In fact, every business is on a digital journey. New technologies such as robotic automation, artificial intelligence (AI), machine learning, to name a few can bring many benefits from increased operational efficiency to improved agility and higher employee engagement.

However, digital transformation inevitably introduces more security risks for organisations as their attack surface broadens. And cyber criminals are poised to take advantage of those companies quickly deploying new tools and completing fast upgrades without properly securing systems and defences.

Thinking of digital transformation and cyber security as separate strategies with independent objectives and goals can expose an organisation to significant risks

It is even argued that the digital landscape and the levels of disruption caused by digital transformation are currently proving far more fast-moving than modern cyber strategies. In other words, the new and innovative measures of cyber attacks are outpacing regulations, organisations' strategies and governmental policies significantly. To reduce cyber risk exposure and protect their business, IT and security teams need to ensure security is present at every step of the transformation process. More mature companies have already adopted this approach and are now seeing the benefits, but changing strategic approach isn't always easy. So where should your organisation start?

The key to success in any transformation is to put a comprehensive strategy in place first with clear objectives and a detailed plan. Too often senior management can think of digital transformation and cyber security as separate strategies with independent objectives and goals. However, this can expose the organisation to security vulnerabilities and other significant risks – which can have serious consequences.

To mitigate risks and improve cyber resilience, instead organisations should develop a cyber security transformation strategy. This enables businesses to adopt the latest technologies and transform digitally while also reducing the exposure to cyber attacks. Organisations can even go as far as making security transformation the driver of digital transformation. For example, identifying any areas where vulnerabilities exist within legacy IT infrastructure and putting a security transformation plan in place, which will ultimately drive the wider digital transformation of the business.

This strategy ensures cyber security is as strong as possible before broadening the attack surface further, rather than the typical reactive approach whereby business and technology transformation are the priority and security is only considered afterwards.

Most decision makers at board level understand the concept of a digital risk. However, many lack the widespread technical knowledge required to predict and imagine how damaging a cyber attack can be. In 2020 data breaches cost UK companies an average of $3.88-million per breach, but that is not the whole story. Poor security can significantly damage reputation, leading to lower employee morale, lost customers, partners and suppliers.

To protect organisations, it is critical that the management team understands the importance of cyber security transformation. The C-Suite needs to be onboard and engaged with the idea of putting security transformation first, ensuring the best possible future-proofed outcome. Cyber security should be seen as enabling innovation from the top-down, not holding it back and should form a critical part of the initial design of any transformation strategy.

Cyber attacks are evolving every day and it can be hard to stay on top of and maintain a clear understanding of the latest threats. This problem is only exacerbated as organisations transform and the digitalisation of business introduces new attack surfaces and associated risks.

Security teams need to identify any dangers that transformation may pose before beginning any transformation journey. For example, shifting business operations to accommodate more home working can increase the changes of a data breach occurring if user credentials are poorly managed and protected, authentication for devices or systems isn't sufficient and data leak prevention is not in place.

Similarly, the digitalisation of and increased connectivity between supply chains could pose a danger to businesses. Cyber criminals like to take advantage of smaller vendors with poor security to gain access to larger organisations and, unfortunately, many don't find out they've been a victim until it's too late.

The cloud is also another common transformation area that's highly targeted, particularly as organisation rush to accelerate adoption of public cloud solutions. Poorly configured (and managed) cloud-based infrastructure can become an easy target for hackers and data can be compromised, stolen or services severely disrupted if an organisation does not protect its cloud data.

> **IT IS EXPECTED THAT AS MUCH AS 65 PERCENT OF THE GLOBE'S GDP WILL BE DIGITALISED BY 2022**

Finally, the rise of the Internet of Things (IoT) can increase security risks as more devices connect to the network, again increasing the attack surface. More sensitive data is on display, vulnerable to large-scale attacks. Attackers have also started using artificial intelligence as their weapon, allowing them to make human-like attacks that can easily bypass security checks looking for automated activities.

Cyber security transformation means adopting a zero-trust philosophy whereby each person, device or system connecting to the network and business cannot be trusted. This means authenticating and authorising based on all available data points, utilising just-in-time and just-enough-access to limit user access and using analytics to drive threat detection. This improves cyber resilience while also communicating the value of security transformation to the broader business.

Traditional tools such as anti-malware software and spam blockers are still important, but these need to be combined with proactive tactics, such as threat hunting, staff training and ethical hacking to ensure any vulnerabilities are identified and mitigated immediately.

At the same time, organisations need to be mindful not to just keep investing in more and more security technology and tools at each stage of their transformation. Doing so can mean there is little integration between tools and gaps in the coverage they offer, which could introduce new risks. Similarly, many tools can produce false positives or benign positive threat alerts, leading to fatigue and alert blindness. Security teams need to ensure they conduct thorough research before embarking on a transformation to ensure that new technology does not impede security. Often, the right solution can help to consolidate security tools and increase the ROI of security operations while also strengthening cyber resilience through transformation.

A Managed Detection and Response (MDR) solution can be instrumental in facilitating a cyber security transformation approach. MDR combines human analysis, artificial intelligence and automation to rapidly detect, analyse, investigate and actively respond to threats and can be deployed rapidly and cost-effectively as a fully outsourced service or via a hybrid SOC. It helps to

develop a reference security architecture that enables organisations to safeguard on-premise and legacy systems, cloud-based infrastructure applications and SaaS solutions, while also protecting and responding to new security and user identity threats as well as reducing cyber risk and the dwell time of breaches.

As businesses innovate and transform, so should security teams. Teams that need to be flexible and seen as an enabler and promoter of change need to be more engaged in business planning and application development to effectively manage cyber risks and work closer with developers who rarely view security as their top priority when deploying new features.

CYBER ATTACKS ARE NOW OUTPACING REGULATIONS, STRATEGIES AND GOVERNMENT POLICIES

Team skills should also be considered and evaluated. Organisations may not have the skills in-house to accommodate certain areas of transformation and in this case, it makes sense to engage the support of a third-party. However, a security architect should be engaged early in the project lifecycle to benefit from robust analysis and ensure the correct decisions are made, tracked and traced from beginning to end.

A cyber security partner can also help you understand the interdependencies across your IT estate, identify risks and suggest best practice, as well as legal and regulatory obligations to ensure you continue to be able to withstand a range of cyber attacks throughout your transformation.

Any third party should act as a strategic partner working together with the organisation to understand the interdependencies across the IT estate, identify risks and improve cyber resilience.

Finally, other people within the business, not just security colleagues, play an important part in mitigating the risks of cyber attacks. Human error is still the most frequent point of failure so implementing an internal security awareness strategy, clear policies and encouraging honest, open communication is key in ensuring better personal security. Organisations need to promote secure culture where colleagues are reassured it is OK to come forward when something goes wrong.

Any businesses on a digital transformation journey will undoubtedly face cyber security challenges and threats. These risks, however, shouldn't stand in the way of innovation and potential growth. Security teams need to evolve their strategies and decision-making processes to protect the business, deliver results and secure assets, all while helping the organisation remain compliant with relevant legislation and regulations.

By adopting a cyber security transformation approach organisations can thoroughly and efficiently reduce their cyber risks, even as the possibility for cyber attacks increases exponentially. Businesses will be better placed to identify and respond to cyber attacks, while reaping the benefits of transformation. There will be less chance of operational obstacles during transformation, increased protection even in complex infrastructure and businesses can be confident that their technological environments can withstand a range of cyber attacks even as their attack surface grows.

Organisations that are willing to adopt a more proactive approach to their cyber security operations – by implementing a robust cyber security transformation process – will reap the benefits of a stronger, structured system for managing, isolating and reducing threats. It will be those companies that don't leave security on the side-lines who will win in the long run ●

Martin Riley, Director of Managed Security Services at Bridewell Consulting, joined the company in 2021 and is responsible for leading the continued growth and scaling of Bridewell's Managed Security Service portfolio, including the Security Operations Centre (SOC) and Managed Detection and Response (MDR) service.

Human error is still the most frequent point of failure, so implementing an internal security awareness strategy is absolutely vital