CSPs enable users to store, access and share their sensitive data and content, adding extra layers of security across the enterprise

Picture credit: Towfiqu Barbhuiya

A HOLISTIC APPROACH

Dylan Border *explains why creating an organisation-wide culture of defence holds the key to strong security performance*

Results of a recent pwc survey reveal that 27 percent of global CFOs have experienced a data breach in the past three years, costing their organisation more than $1 million. Companies are under increased pressure to protect their business from threats that could cause extensive financial and reputational damage. Cybersecurity is no longer a 'nice-to-have' – it's business critical. As a result, more customers are interested in how their content and data are being secured. And while many are making progress, some are still playing catch up.

Organisations are facing threats that are constantly evolving and becoming increasingly sophisticated. Hackers are relentless in their search for any gap in a company's security armour. Unfortunately, security is only as strong as its weakest link, and it only takes one insider threat to jeopardise everything. No longer just a passive focus for an IT department, cybersecurity requires organisations to create a defensive and scalable model to managing their policies and technologies that is applied holistically across the whole organisation.

The trend towards remote work has been replaced by a hybrid model, in which many employees work from home part of the time. This has ushered in the rise of bring your own device (BYOD), which means employees need to be more savvy about security.

At the same time, workers are faced with managing an ever-growing variety and volume of content – from office documents to images and videos. With users often struggling to find internal tools that are up to the task and that fit their work styles, it's only natural that their own device might fill this void.

So, while remote working provides greater flexibility, its impact has some negative implications. Introducing hundreds, of employee-owned devices into a company's network drastically increases the risk of a cyber-attack and inadvertent insider threats.

Employees are often using their own devices out of convenience and habit, rather than with any malice in mind. They are simply seeking a work experience equal to the one they have in their day-to-day lives.

It's clear that education is key when it comes to ensuring workers are savvy about the risks. Gartner predicts that: "by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents." Even with the best of intentions, it is impossible for an organisation's IT team to defend against all variables, all of the time. Cybersecurity measures must extend beyond the realm of the IT department and reach every employee in the business – regardless of where they and their connected devices are working from. So, what does this actually look like?

An organisation must ensure that staff are up to speed with best practice security measures and threats. Many organisations we work with are constantly playbooking and running tabletop exercises to address security vectors, while some also offer bug bounty programmes to help cover as many angles as possible, using resources beyond their internal teams. However, the variables of breaches and exploits are endless.

The key to strong security performance is to develop an organisation-wide culture of defence in which all employees are invested and take a proactive role. From the marketing team to the finance department, employees must understand not only why cybersecurity tools and processes are essential, but also how to identify a potential threat and what action to take. This shift heralds a culture change that requires constant and consistent training and education, as well as support and investment at the most senior levels.

Cybersecurity is a careful balancing act. If implemented improperly, it can be incredibly disruptive to a business. Too many security controls can prevent employees from carrying out their role effectively. However, too little security can spell disaster.

Above all else, IT leadership must consider what security approach works best for their organisation. Zero Trust may be too limiting for some organisations, either through the resources required to truly implement it or the management of it once in place. First and foremost, senior leadership must both understand and agree on the organisation's overall approach to security. They must determine what the structure will look like, and how it will be managed. Then, adequate cybersecurity budgets must be allocated not only to developing and onboarding the right technology, but also towards running continuous training programmes across the organisation.

Over the last few years, organisations have invested in content services platforms (CSPs) to enable employees to collaborate effectively whether they are office-based or working from home. CSPs enable users to store, access and share their sensitive data and content, while also boosting productivity. They also add extra layers of security across the enterprise.

CSPs employ several tactics to keep data secure from the moment it enters your organisation, to the moment you decide that you no longer need access to it. For example, automated processes can be set up based on predetermined rules to mask, delete, encrypt or archive records and therefore protect them from unnecessary exposure. Businesses can enable workflow automation to significantly reduce the number of human contacts data points are exposed to, thus improving both accuracy as well as security. And redundant configurations can mitigate the potential impact of ransomware attacks.

Essentially, CSPs allow businesses to automate and secure internal data and documents, by giving the right people access to the right records, with historical monitoring to help audit this access, if it's ever needed.

In order for cybersecurity to stay top of mind, organisations must develop training programmes that employees engage with regularly. In doing so, staff will always have fresh, up-to-date knowledge on the importance of security, as well as a robust understanding of the types of new attacks out there. In 2023, we are seeing a focus on ransomware and supply chain attacks, as well as the ongoing prevalence of phishing attempts. Unfortunately, security is never a case of 'once and done' – attacks are constantly evolving, and team members' knowledge must develop at the same rate.

IT LEADERSHIP MUST CONSIDER WHAT SECURITY APPROACH WORKS BEST FOR THEIR ORGANISATION

Ideally, training should extend beyond the hypothetical, to include realistic attack examples. For example, in best-in-class organisations, non-technical teams are exposed to simulated attacks in order to find out how employees would deal with a real-life scenario, such as a phishing attempt. These 'drills' prepare a user for a genuine attack, and they also offer security professionals invaluable insights into weak points across the business. This information should be used to inform future training programmes, to ensure that they are as robust and up-to-date as possible.

As part of the training, trainers must make it clear how to properly report suspected attacks. The company's incident response plan should include expected timeframes for reporting a potential threat, as well as any details required to assess the risk level. Employees should be made aware of their legal obligations to report a threat, such as a suspected data breach, within a timely manner.

In order for employees to take security seriously, and feel accountable for maintaining appropriate standards, many businesses include employees' cybersecurity obligations within their job descriptions. This sends a clear signal that security is their responsibility, and they must take a proactive approach upholding the business's security agenda.

These requirements generally cover password protocol; adhering to multi-factor authentication policies and following any other digital hygiene measures that are described in the company's cybersecurity guidelines. It is also likely to include a requirement to follow cybersecurity training and education courses regularly.

For organisations enabling BYOD, employees should also be made aware of the organisation's BYOD policy as part of their onboarding. These policies will likely cover device maintenance; approved access to applications and functions; sharing of company documents; installation and regular updates of antivirus software; use of firewalls and what constitutes appropriate personal use of the device.

THE KEY TO STRONG SECURITY IS TO DEVELOP AN ORGANISATION-WIDE CULTURE OF DEFENCE

Beyond continued training for non-technical staff, it is also crucial to ensure that your cybersecurity team always has access to timely information about the changing security landscape. As well as new types of attacks emerging, security teams must keep a pulse on the latest external validation points that may be required by customers, such as ISO standards and HITRUST compliance.

Cybersecurity is a rapidly evolving industry, with new trends and technologies constantly emerging. In 2023, hot topics are AI and the vast security opportunities it affords, continuing to secure remote workers and how to best secure this model into the future, as well as Zero Trust. Without deep knowledge of these concepts, it can be difficult for security teams to advise the business on where to invest, and what is even possible to achieve within their specific organisational framework.

Technical teams must keep their knowledge updated to be able to advocate for the most appropriate course of action for their business. Security professionals should be encouraged to attend conferences and undertake relevant courses and certifications.

In 2023, almost half (48 percent) of UK organisations say a "catastrophic cyber-attack" is the top risk scenario within their business. Every day, cyber threats are growing in severity and frequency. It is therefore unsurprising that cyber security budgets have increased in recent years, as senior leadership becomes more aware of the risks posed by failing to invest in security. Within my work, we are seeing an increasing number of companies placing security at the top of their agenda – and for good reason.

While a rise in interest in this area is a positive step, we must also acknowledge that creating a strong cybersecurity defence takes time. Some leaders are under the impression that simply hiring in new and experienced team members means they can take their eye off the ball. However, without proper continued support and contextual guidance, new security staff can be limited in their understanding of the organisation's software, system and processes. Even the most talented teams cannot secure what they do not understand.

For these reasons, an organisation-wide approach to cybersecurity is essential. Senior leadership must not only allocate budget to the programme, but they must also enable their IT teams to work collaboratively with the entire business. By implementing effective CSPs, they are able to ensure that content and data is protected throughout its life within the organisation's estate. Finally, they must empower staff to play their crucial role in securing the enterprise. For organisations yet to embrace this holistic way of working, there has never been a better time to start ●

Dylan Border is Hyland's Director of Cyber Security. He is responsible for leading the Cyber Security Operations and Governance, Risk & Compliance teams, which facilitate the secure operations of Hyland's enterprise networks, systems, and business processes.

The increase in working from locations outside of the office has intensified the need for employees to remain savvy about security

Picture credit: Glenn Carstens Peters