REAL-TIME THREATS

Emily Heath *reveals why your organisation is underestimating the cybersecurity challenge*

Cybersecurity threats are nothing new. Every year, it seems industry experts warn it is time to take security more seriously. For the most part, organisations have responded to those warnings. Once solely managed by IT, cybersecurity is now a C-level concern that is central to the smooth operations of organisations in every sector. Despite the increased focus, many businesses are still underestimating the scale of the challenge.

Today, threats are constantly evolving in both volume and complexity. Meanwhile, increased digitisation means the range of potential attack vectors is also greater than ever before.

The reality of cybersecurity is that it is not enough to merely adopt the latest solutions and maintain them. A strong security posture depends on the ability to track trends and respond to them, evolving cyber protection in line with real-time threats.

Cybersecurity is a multi-faceted challenge, and one with serious consequences should organisations get it wrong. Here are some of the key issues that Chief Information Security Officers (CISOs) need to consider to ensure their cyber provisions are capable of defending against modern threats.

The ever-changing nature of modern cyber threats means a sound, organisation-wide defence strategy is central to effective operational and business performance. The best IT security teams develop a collective understanding of how the business runs, as well as the technical landscape of infrastructure, networks and applications.

Together with senior leadership, IT needs to evangelise that security is now a way of working that includes everyone – it needs to be built into the DNA of the organisation. However, it is important to recognise that cybersecurity is about more than just internal provisions. Too many security professionals do not pay enough attention to external factors such as third-party and supply chain risk as well as the remote nature of doing business globally where the COVID-19 crisis has revealed why this can be a problem.

In a matter of weeks, almost every organisation had to transition entire workforces to remote offices, including the use of VPNs to access systems. Expanding the digital perimeter of an organisation, from centralised office environments with dedicated security architecture to a disparate network of hundreds or thousands of staff devices, has exponentially increased the security risk

Cyber criminals are already seizing the opportunity. According to IBM's cybersecurity division X-Force, March to May 2020 saw a 6,000 percent increase in pandemic-themed spam, some including phishing attacks. These efforts are getting harder to spot. Phishing emails were once ridiculed for their outlandish narrative and creative spelling, but they have become much more sophisticated and convincing in recent years. Beyond email, COVID-19 related domains are 50 percent more likely to be malicious than other domains registered during the same time period.

To protect their organisation**,** cybersecurity professionals need to start to develop a better understanding of their operations, what their most sensitive assets are and where they are located. Many make the mistake of applying the same cyber controls across the board, wasting resources protecting inconsequential assets while under investing in areas that require the most protection.

A STRONG SECURITY POSTURE DEPENDS ON THE ABILITY TO TRACK TRENDS AND RESPOND TO THEM

The next stage is to identify where the biggest vulnerabilities lie. Visibility of every device connected to the corporate network is essential, as well as the areas of the digital estate representing the greatest risk. Attackers are always on the hunt for gaps, like missing patches or outdated software, so it is vital that security professionals are able to identify and remediate vulnerabilities before they are exposed.

These kinds of capabilities depend on proactive monitoring of the business environment, especially when it comes to the assets identified as high priority. Further, regular testing of controls, mitigation strategies and resilience will ensure you are ready to respond if monitoring flags any concerns.

This kind of vigilance also needs to extend beyond your company's four walls. As modern companies become increasingly digitised, every organisation is now an ecosystem, integrating with numerous others across value chains. Selecting trusted partners and establishing information sharing processes with them will go a long way towards minimising the risks associated with a growing landscape of potential threats and entry points.

COVID-19 is both driving the volume of spam and phishing as well as increasing employee susceptibility to them

Cybersecurity is not just about tech, it is about relationships. It is also about understanding human weakness and incentivising the kind of behaviours that will keep data and systems safe.

Not only is COVID-19 driving the volume of spam and phishing, it is also increasing employee susceptibility to them. From anxiety about the pandemic to the toll of extended social distancing, everyone is feeling additional pressure right now and stress can lower our guard to tactics like phishing. It is imperative that every employee, regardless of their role, understands their responsibility to safeguard the organisation's cybersecurity.

It is worth considering how simulated attacks can be used to train staff and ensure vigilance against the increased threat. Simulated attacks should be done with the employee populations where specialists dedicated to security awareness and education are useful. Its also important to test your incident response plans and your teams' ability to detect and respond to cyber threats, as the saying goes – make the practice harder than the game!

On a related note, cyber skill shortages are another issue requiring urgent attention, particularly when it comes to skillsets like ethical hacking. Organisations need to build strong talent pipelines and be prepared to support development of these skills. External support from specialists and employment organisations like Year Up can help set this in motion.

At DocuSign we are building a varied talent pipeline across from non-profit internships to higher education candidates as well as working actively within the security community to attract and retain the best talent. Our employees all receive training and constant engagement from our trust and security team.

Addressing a long-standing HR issue can also help drive results – the lack of diversity in cybersecurity. Building more diverse teams with varied skill sets, cultures, races and genders will increase the likelihood of having the strongest, most holistic and creative security strategies in place. Diverse teams are creative teams, and in cybersecurity, we need all the creative muscle we can get to solve the most complex cyber problems.

With data volumes increasing daily, the integrity of that data is critical to turning it into a useful asset for the business. Advanced analytics and AI are two of the most promising methods of translating the avalanche of data organisations face into value—but only if the data is reliable and of sufficient quality.

> IT IS NOT ENOUGH TO MERELY ADOPT THE LATEST SOLUTIONS AND MAINTAIN THEM

AI provides the insights for security teams to focus their attention on addressing the most pressing threats. These tools help tackle tasks like curating and correlating a multitude of intelligence sources, identifying trends from proactive monitoring and analysing real-time data feeds faster than a human could ever process. However, data quality issues, like consistency, integrity, accuracy or completeness, have a detrimental impact on AI performance.

Addressing this issue requires a human solution. When it comes to data collection and handling, people need to understand what is expected of them. These expectations need to be communicated in plain language. People don't like what they don't trust, and they don't trust what they don't understand, so clear communication and transparency is absolutely key.

Every organisation today needs to implement common sense, easy-to-understand frameworks, policies and standards or they risk undermining the trust in the data they hold.

A HOLISTIC APPROACH

Effective cybersecurity is similar to having a good agreement process in a lot of ways, requiring a more holistic approach to people, operations and technology. Without big-picture thinking, siloes emerge, ineffective processes become commonplace and risks multiply.

Businesses cannot afford to take this lightly because the penalties for failure are significant. On the regulatory side of things, the EU's GDPR gives authorities the power to issue fines of up to €20-million, or four percent of an organisation's annual turnover, whichever is higher.

Reputationally, breaches can be costly too. According to a report by the Ponemon Institute, 36 percent of the overall cost of a breach is in loss of business as customers and prospects react to the news. A well-executed communication response, prioritising the timely and transparent sharing of information, can mitigate some of the brand damage, but this will only go so far.

The best response to the threat of a cyber attack should not be fear or caution. The range and severity of attacks have increased, but the tools built to guard against these attacks are stronger than ever. To appropriately defend against modern cyber threats, you need an effective strategy, one that invests in the people, skills and technology required to get in front of the problem. It's an opportunity to align company-wide processes, employees and data resources in a way that will not only protect against threats, but actively move the business forward ●

Emily Heath was appointed as DocuSign's CISO in 2019. She currently oversees a wide range of strategic and operational elements relating to DocuSign's global business – including information security, application security, trust services and physical security.

VPNs have become increasingly popular as more team members are forced to work from home