The RSA Conference 2021 highlighted the importance of remote working and data privacy for security vendors

June 2021

Igor Babić

The official theme of the virtual RSA Conference 2021 was 'resilience'. The time between last year's event and this one has been marked by the COVID-19 pandemic, so it was no surprise that many of the sessions at this year's conference focused on the resilience of people, processes and technologies in light of significant changes in working patterns.

Resilience is usually perceived as the ability to recover after something bad has happened, but the key messages from the event related to being proactive in cyber-security efforts – detecting threats before they cause harm – rather than on incident response. We noted three themes during the keynote sessions that are of particular relevance to vendors that supply cyber-security to solutions to the small and medium-sized business (SMBs) market – we discuss these themes in this article.

Organisations need to proactively refresh their cyber-security technology stack and make sure that it is well-integrated

Wendy Nather of Cisco and Wade Baker of the Cyentia Institute delivered a keynote session that explored what makes organisations' security programmes successful (that is, what is the link between employing certain practices and favourable security outcomes). This talk was based on a survey of over 4800 businesses worldwide, from a variety of industries and of a range of sizes.

Our two key takeaways from this session were as follows.

- 'Proactive tech refresh' and 'well-integrated tech' are two key practices that lead to favourable security outcomes, particularly in SMBs.

- What matters most in an organisation's security strategy varies by business size. For example, the ability to identify top cyber risks is not at all correlated with the security success of organisations with fewer than 1000 employees, but is an important driver of favourable outcomes for larger enterprises. Larger organisations face more threats, their cyber-security estates are more complex to manage, and it is therefore more important for them to understand what they are defending against so that effective prioritisation of tasks can take place.

These findings are logical, but many organisations (and in particular SMBs) cannot afford and/or do not have the appropriate resources/skills to proactively refresh their cyber-security solutions and make sure that the technology they use is well-integrated.

Analysys Mason's survey work has shown that the vast majority of SMBs think that they are satisfactorily protected against cyber threats, but well over half of such organisations do not frequently update/add security-related software and services, and do not regularly conduct IT security assessments.

This has the following implications for security vendors that are targeting SMBs.

- Vendors that offer SaaS/cloud-based solutions and have a wide offering are best-placed to deliver favourable security outcomes. A SaaS model would allow for automated provisioning of updates, which would simplify security operations. A wide offering would enable a good integration of technologies that protect fixed endpoints, mobile endpoints, networks and data.

- Vendors should increase their focus on partnering with managed service providers (MSPs). SMBs that lack resources and/or skills internally are increasingly seeking help from MSPs. Another survey conducted by Analysys Mason has shown that over half of organisations with 50–999 employees in Australia, Canada, the UK and the USA have started using, or increased their use of, managed services in response to the COVID-19 pandemic.

Privacy will become a central component of organisations' cyber-security efforts

Vasu Jakkal of Microsoft argued in another keynote session that privacy should be a key component of a strong security strategy. More than ever before, people are thinking about the businesses that they interact with and questioning whether their data is in safe hands. Jakkal noted that "trust will likely be a defining characteristic of business success in this decade". This implies that security professionals will need to pay special attention to privacy in their work. Privacy, in an organisational context, has the following two key elements.

- **Data protection**, which entails protecting personal and organisational data from unauthorised access and intentional or unintentional destruction, modification or disclosure. Encryption and data loss prevention (DLP) software are examples of related solutions, and these are generally managed by security/IT teams within organisations today.

- **Data privacy**, which entails the handling, processing, storage and use of personal information in accordance with regulations and ethical standards. This is increasingly dealt with by security/IT teams. Also, organisations are trying to ensure that a wider range of employees are knowledgeable about data privacy risks and related requirements.

This focus on privacy in the business world means that security/IT teams will generally no longer only be responsible for keeping unauthorised individuals away, but also for making sure that those who are authorised to have access are acting in accordance with their rights. Security vendors should therefore adapt their offering to changes in the scope of security professionals' work and generally increase their focus on privacy-related issues in marketing materials. This shift – to privacy being a key focus – is also helping to expand the size of the addressable market for security vendors.

The shift to remote working during the COVID-19 pandemic has accelerated trends that already existed in the cyber-security market

A number of keynote sessions at the conference addressed changes to working practices caused by the COVID-19 pandemic. Our view (and that of some of the speakers) is that these changes mostly represent an acceleration in trends that were present before the pandemic. For example, the popularity and acceptance of remote working has slowly increased since the introduction of mobile devices and the adoption of cloud-based business applications (such as Salesforce) has also been growing steadily for many years. The pandemic has just accelerated these trends (most notably the adoption of cloud communications). To capitalise on this, cyber-security vendors should continue to shift their solutions to the cloud too, and make their solutions easy to manage remotely and by third parties (such as MSPs).