White Paper

Cyber Security Predictions 2021

Looking forward to next year in cyber security

Huntsman®
Defence-Grade Cyber Security

Introduction

> This annus horribilus, with almost 12 months of the COVID-19 pandemic has touched almost every aspect of our lives; and it's not done yet.

Before looking to anticipate the events in the year to come, it is normally quite interesting to look back and review the predictions made this time last year. 2020 however, has meant some less expected events and outcomes. This annus horribilus, with almost 12 months of the COVID-19 pandemic, has touched almost every aspect of our lives; and it's not done yet.

Our predictions this year have to be made in the context of that ongoing health crisis. So much has changed that some of the predictions we now make for 2021 might have seemed almost ridiculous just 12 months ago.

2020: An unpredictable year

The MSSP sector grew during 2020, resulting from the need for more flexible remote working arrangements everywhere. With the majority of employees, including security personnel, working from home the benefits of MSSPs with their reach and ability to remotely manage and protect IT assets have been widely sought after. Arguably even more than anticipated.

We've also seen an increase in attention being paid to "RegTech" or the digitalisation of compliance processes – either through the enforcement of controls or the management and monitoring of them. Again, the pandemic has tested traditional audit and compliance functions due to limited access to many data centres, offices and suppliers where data is stored or processed. This has meant an increased interest in the automation of governance and audit processes.

Our prediction that security risks would become reputational rather than financial, has been hard to judge in this environment. With all the other worries people have, a business losing data or suffering a breach just isn't their biggest personal or corporate concern; although regulators have continued their efforts to ensure an adequate level of security governance is maintained. In Australia definitive "cyber security obligations" for owners and operators of an expanded Critical Infrastructure sector are under discussion and the ICO in the UK finalised a significant penalty on British Airways for a breach of GDPR. Both confirm the slow increase in enforcement efforts. Governments everywhere have warned of increased cyber security vulnerabilities and risks of attack because of overall disruption across world economies this year.

> "Again, the pandemic has tested traditional audit and compliance functions due to limited access to many data centres, offices and suppliers where data is stored or processed."

Lastly, we expected cyber risk management information to be integrated more broadly into business strategy, reporting and executive accountability. This has been visible, in some respects, over the last year with some jurisdictions better articulating the link between cyber security efforts and D&O responsibilities. In the related area of supply chain risk (in which we predicted evolution) several government programmes, such as the DISP programme in Australia and the CMMC scheme in the US have increased defence industry focus on "infection by 3rd party risk", with the introduction of standards and assessment frameworks for the management of cyber risk performance of supply chains.

COVID-19

Unfortunately, no predictions paper cyber or otherwise, can ignore the march of COVID-19 across the world. Some countries have been and continue to be affected quite badly; such as the US, Europe and the UK. Others, like Australia and Japan have had greater success managing the virus spread.

What we have learned however, is that while not wishing to trivialise the events of the last 12 months, there is a sense of familiarity here for people operating in the cyber security sector. There is no set and forget solution, emerging vaccines will not be a universal silver bullet; we need to keep sharing threat information, keep executing on our risk management plans and monitor our mitigation efforts. The health and economic stakes relating to cyber security are obviously not as high as those for COVID-19 but there are certainly parallels and lessons to be learned here. Risk management and scenario testing pay dividends.

As this report is prepared, the UK and much of Europe is emerging from a second round of COVID-19 induced social restrictions and the virus is still accelerating in the US. Australia looks to have come out of the back of its second spike. But there is no room for complacency and while the vaccine and ongoing diligence will certainly enable us to return to some level of normality as 2021 progresses many things, including the way we work, are likely to have changed forever.

2021 Predictions

Home working is the new default, but it will continue to compound security risks with breaches, loss of data and other security failures in organisations where security vigilance has been allowed to drift

For many people "WFH" has been the reality for much of 2020 with many businesses now having a largely home-based workforce.

Past barriers to this, in terms of available technology, personal preferences or management reticence, were largely removed as part of the public health effort to contain COVID-19.

Already, this is changing the way business is thinking about office space, hot desking and office amenities more generally. COVID-safe working environments will be the norm for some time yet and even beyond that work patterns will change

As a result of this change there are three clear security implications for 2021:

1. Insider risks will increase

Moving information and IT assets beyond the office security perimeter will become more common. The limitations of physical controls on access, printing out data or introducing removable media in an effort to maintain operational efficiencies will not seem so unreasonable anymore.

Further, some controls aiming to prevent data theft might have been made almost irrelevant by the rush to support home working. The demise of security solutions based at the network gateway will be observed, and changed risks resulting from the use of personal computers for work purposes will be evident too, with a lack of surety around patching levels, anti-virus and access control.

Consequently, we predict that malicious insider incidents will rise and we suspect that they already have. Organisations are just unable to detect these activities yet.

2. Endpoint compromises will become a more pressing threat

The threat of the end point being compromised by a hacker, perhaps as a result of a phishing attack or drive-by download, has increased hugely as a result of fewer controls between the systems in question and the Internet.

Email will still pass by gateway protections, but web browsing and personal email use are more likely to be threat vectors on home-based systems than on better protected work systems. Attacks that were once thwarted by a trusted network are now invisible.

While "Zero Trust" remains universally acknowledged as a desirable ambition many businesses still rely on the network itself as a line of defence. This is a line of defence that in 2020 and 2021 is undoubtedly weaker – and the effects of that will become apparent.

3. Data is everywhere – and harder to protect than ever

Increasingly data is everywhere, and in many cases less well protected than pre-2020 because of some of the less robust WFH security solutions deployed at speed and for convenience at the height of the pandemic.

As a result incidents of data loss (i.e. theft), corruption or failure (e.g. from deletion) will continue. Hastily constructed cloud-based shared storage areas, corporate email attachments littering the temporary files of domestic PCs and reports extracted from business application systems sitting in personal web-based email systems, are just some of the probabilities.

Companies will have to get to grip with better security management of these types of problems as working remotely remains the norm, rather than just a response to a crisis, or we'll see more security failures, breaches and exposures of sensitive data.

Third party assurance and audit approaches will transform to reflect the post-lockdown business working environment

Auditing and measuring the effectiveness of your own security controls is hard at the best of times. For companies with a large number of third party suppliers, evaluating their security posture is even more challenging. Do you even know the current level of your residual IT risk? Does your cyber insurance underwriter?

Up until now approaches have varied, but none are perfect. Questionnaires can be unreliable and lack objectivity; interviews are logistically complex and resource intensive; and external bureau-based approaches (there are several on the market) while cheap, lack rigour and in the worst case they completely miss-report the true nature of risk.

The pandemic has meant that most of these techniques are no longer appropriate and are overdue for transformation. Businesses don't yet know how effectively the suppliers in their supply chains have managed their security during this turbulent year.

Under lockdown, anything involving manual inspection has been virtually impossible. This together with some of the issues already discussed has led to issues of trust and questions of reliability about 3rd party security controls. They remain a significant source of security threat. Too much time has elapsed and circumstances changed for some historical audits to be relevant.

As a result, 3rd party risk management processes and procedures will come under renewed focus in 2021 as digital transformation of security and compliance begins in earnest. More broadly, organisations will look to better understand the cyber security posture of their enterprise and its vulnerability to attack. They will use this information to inform (i) operational teams of risks that need mitigation as well as (ii) senior executive and boards of the status of their cyber security efforts.

As counterparty trust and reliability are key to the success of digital transformation it will mean the shift from less systematic manual audits and questionnaires, to reliable and automated processes, through ultimately, to continuous security control monitoring and reporting.

> “Do you even know the current level of your residual IT risk? Does your cyber insurance underwriter?”

Video conferencing services become a target for hackers and a route through which losses of data and privacy breaches can occur

2020 has been a year where face-to-face meetings were replaced by Teams, Zoom, WebEx, Slack and others. The resulting massive scaling of these services to meet the demands of universally replacing in-person discussions tested our patience and for many the security of our communications. "Zoom bombing" was added to our business lexicon and almost every meeting includes the phrase "You're on mute."

Our prediction for 2021 is that at some point one of these services, or someone's account on one of these services, is going to fall victim to hackers. And that business will have its recorded secrets leaked in audio/video form through passive interception or the recovery of past meeting files.

The ongoing improvement of the medium and our year long education of its strengths and foibles will ensure that for all but the most sensitive meetings, its use will continue to grow.

Managed security services and cloud hosting will accelerate driven by the need for cost savings, a refreshed view of risks and the increases in remote working

An increasing number of companies have adopted cloud hosting and invested in managed security services, as many of the perceived concerns about those services have fallen away during the last 12 months. Past barriers to adoption included:

- A desire for systems to be within reach or close to the IT and security teams
- Wanting IT facilities to be located in the same place as the user population
- Reticence to perform oversight if a third party is involved in storage/processing

With users working out of the office and data now everywhere, the barriers to utilising cloud IT delivery have dropped away.

If IT and hosting are remote, why should the security operations function be in the office? And if they are remote, why manage the team yourself when you can achieve the same outcome with a service from a specialist provider?

"In house" managed security services in various forms will continue to grow through existing and emerging vendors. In 2021, businesses will learn from this past year so we expect a sharp increase in growth in external hosting of systems and the security controls that protect them.

MITRE ATT&CK will continue to grow in adoption – by vendors, end-users and service providers

We've seen widespread adoption of MITRE ATT&CK across both the end user, MSSP and vendor communities in 2020 and this is a trend we see gathering further momentum.

The ATT&CK framework is a knowledge-base of cyber attack tactics and techniques. The security industry is not short of standards and checklists, with already too many to choose: NIST, SANS, ISO, PCI, ISACA, ISF and Essential 8. What sets MITRE apart is that it provides an attack taxonomy that groups the elements of an attack by type and intent to enable ease of investigation and prioritisation by analysts. It is extremely useful for categorising attacks, so security operators can understand their nature and status of an intrusion. This will enable all SOC operators to categorise their attacks according to a common lexicon and even help with attribution or anticipate what might happen next.

The vendor community will continue to add MITRE ATT&CK support to security tools to assist SOC operators in the contextualisation and threat investigation processes. By categorising SIEM events using the ATT&CK matrix, analysts will be able to identify the nature of attacks, assess their severity and intent and pre-emptively hunt for other contextual events.

In saying that, not all MITRE Screens will be the same. Ensuring that you can look at your SOC data through an ATT&CK lens is key to being able to leverage the true power of the threat information for the effective investigation of your threat environment.

The continued rise and evolution of UEBA and the migration of EDR technologies into a more advanced and comprehensive XDR form

In line with the above advances in MITRE's prominence we'll see a corresponding consolidation in the UEBA/EDR/XDR space.

UEBA (User and Entity Behaviour Analytics) has been a staple of SIEM technologies for years, the recognition that data gathered centrally can be analysed using behavioural techniques is well accepted. This has led to the additional emergence of end-point solutions that aimed to mimic UEBA capabilities with endpoint analytics based solely at the workstation/end point.

Of course, both types of solution have merit. 2021 will therefore see cautious buyers assessing their existing security insights against what these newer end point solutions can offer. Buyers are increasingly aware of the system loads some monitoring solutions put on their environments. No one will deploy a complex endpoint solution if centralised solutions can offer equivalent protection and the growing complexity of their end-point configuration causes problems. The market will spend heavily in seeking the right balance between the benefits of ready access to end point information and the complexity in adding yet another layer of security functionality.

Cyber security grows in recognition as a vital element of good corporate governance

As a cyber security solution provider, Huntsman Security is also a keen observer of public policy. It does however focus its efforts on cyber security performance improvement which is, of course, one of the many risks faced by enterprises. That said we also recognise that it is increasingly meaningless to talk about cyber security risks in isolation. Industry and more recently regulators have recognised the digitalisation of enterprise; this means almost every aspect of economic endeavour and transactional activity has an interconnection with cyber risk.

It's for that reason we believe the health of your cyber security is an overall indicator of the wellness of your enterprise. Success in the digitalisation of our economy demands reliability and trust relationships between digital partners and counterparties. This expectation is increasingly being monitored by regulators everywhere which means that senior executives and directors will be charged, as part of their corporate responsibilities, with the management of and accountability for monitoring and managing the cyber security posture of their businesses.

> "Success in the digitalisation of our economy demands reliability and trust relationships between digital partners and counterparties."

Already in some jurisdictions, defective cyber security infrastructure or performance is being seen as a failure of corporate governance and board responsibilities. This is a trend, and the continuing vulnerability of individuals and organisations to cyber attack is likely to hasten the growth of legislation and enforcement in the coming 12 months.

Talk to Huntsman Security about your cyber security monitoring and measurement

For a detailed discussion on monitoring and measuring your cyber risk, please contact the appropriate office listed below.

About Huntsman Security

Huntsman Security is the trading name of Tier-3 Pty Ltd. The heritage of our technology lies in delivering a key foundation stone of the cyber security risk management, monitoring and response capability in some of the most secure and sensitive environments within the intelligence, defence and criminal justice networks across the world, where Huntsman Security solutions are deployed and accredited to the highest security levels.

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman