MITIGATING THE CYBER THREAT

The Roundtable Panel included:

ED BENGOA director of post production, ITN

ADRIAN BULL ceo, Cinelab Film & Digital

ZEB CHADFIELD chief vision officer/ceo, The Finish Line

TOBY CLOWES director and head of cyber, Tysers Live

CHARLIE EVATT director and principal consultant, Evatt Industries

PAUL HILLIER director, media, film & tv, Tysers Live

ROB JONES executive chairman, head of media, technology and cyber, Nirvana Underwriting

CHARLOTTE LAYTON co-founder, Racoon

NICK LONG ceo, Salon

TOM MITCHELL co-founder and technical director, Mission

NICK PLATT vice president, Picture Shop UK

SYMON ROUE managing director, Visual Data Media Services

STEPHEN STEWART consultant (TPN UK and EMEA Ambassador)

LOUISA SUTHERLAND-SMITH md, Halo Post Production

Cyber-crime has grown exponentially since 2017. Although much of this discussion comes from a post perspective, most of the content is relevant to all UK media businesses.

On the 27th of February, with the support of Tysers Live and Nirvana, *Televisual* hosted a dinner at the Groucho Club to discuss the challenges for UK post and production around cyber security. The event followed three recent, though all thwarted, ransomware attacks on UK post houses with all three companies reflecting on their experiences to start the discussion.

The panel comprised senior UK post directors,two insurance broker directors, including their cyber expert, an underwriter who specialises in cyber insurance for media businesses, the Trusted Partner Network's (TPN's) UK representative and a TPN third-party assessor.

Insurance companies are at the frontline of understanding cyber security from how to mitigate against a cyber-attack and the importance of a Disaster Recovery Plan (DRP). They are often the first response unit in the event of an attack. The TPN is a trade body formed by many of the largest US studios that publishes security best practices within film and television, recommends security standards and protocols, and certificates vendors and post houses.

This report was collated after the event. There are many reasons for this, from not wanting to compromise any one of the panel through reported speech and so that they could collect their thoughts with the benefit of having attended the discussion. But above all cyber-crime is rarely covered within UK media and the intention of this report is to further understanding across UK production and post and so stimulate conversations about what measures might be taken to protect both companies and production assets and how working together, cyber security can be more effective.

TYSERS LIVE

Tysers Live, a new division of Tysers Insurance Brokers, brings together our expertise across the media and entertainment industry under one brand. We are proud to boast a team of some of the world's most passionate, knowledgeable and skilled risk and specialty insurance professionals to manage the many issues facing our clients today.

As market leaders in providing innovative insurance broking solutions to the Film & TV industry we specialise in providing comprehensive insurance and risk management services tailored to the needs of our clients.

We cover all areas of the sector, including media, film, television, theatre, music and events as well as more specific media sectors including freelancers, post-production, VFX, SFX, outside broadcast, facilities and hire companies and we design insurance programmes that are responsive to their emerging and complex needs and requirements.

tysers.com/solution/entertainment-sport/media-film-tv

nirvana

Nirvana offers a comprehensive three-part cyber insurance solution for the media industry comprising:

1. Cyber security assessment and risk management including various levels of client domain and network scanning to identify vulnerabilities.

2. A risk transfer solution, providing our customers with balance sheet protection covering internal and third-party liabilities arising from a cyber event.

3. Incident response, including a 24/7, 365 hot line to trusted and experienced response vendors who have established relationships with Nirvana and our Lloyds insurance partners.

Nirvana has a unique market offer as a long-standing specialist insurance provider serving the global media industry and providing cutting-edge cyber insurance solutions to a broad spectrum of professional firms, financial institutions, retail, healthcare, educational organisations and technology providers.

nirvana-uw.com

This report starts with the experiences of three UK post houses who were recently subject to ransomware attacks. In all three cases, the attacks were repelled and in the discussion our insurance and security experts praised the executives for having implemented and adhering to recommended protocols and for taking robust and appropriate action. In all cases the attacks were through hardware and software vulnerabilities within the corporate network and client assets sitting on other island servers were not at risk. None of the attacks involved protocol failures or on-site physical security issues. They were - as most cyber-attacks are - not directed at a specific organisation but instead on exploiting cloud-facing IT vulnerabilities.



Criminal Record for Apple TV+, digital dailies lab by Cinelab

'ZERO-DAY' VULNERABILITY

Symon Roue The ordeal began early on a Saturday morning just after I had attended a trade show in Miami. Our US head of IT called to say he'd had notifications of servers that had gone offline in our Burbank facility and that he was heading to the facility to investigate. Immediately, he assessed the potential of malware and shut down all access to the network taking the Burbank facility entirely offline.

From that moment onwards began a series of 18-hour days for many of us at Visual Data. Our first step was to call our insurance company. Incredibly, by 4pm that same afternoon, we had a full cyber security team, IT forensics and legal support on a Zoom call. They notified the FBI as well since this had the appearance of a well-known cyber-crime group.

In our investigation, we found these Threat Actors (TA) had left a note and a link leading to their chat window on the dark web with threats and demands for negotiation. We hear and read about these events, but in person, it is a surreal experience for any business leader. Thankfully our cyber and forensics consulting team were experts at these situations and got to work dealing directly with the TA to analyse the issue.

They were able to confirm that, thanks to good MPA security practices and diligences on the part of our internal teams, the TA had failed to get what they were after. They had no customer media files, no internal files, and no files of any value.

In parallel, our team initiated business continuity plans, re-routing traffic and operations to our London facility, flying several teams of people over whilst the IT forensics team started the process of wiping the facility clean.

By Monday we had begun engaging clients' infosec teams, rescheduling works and communicating contingency plans. Our clients were very supportive, many of which had been victims as well, so they knew the drill. Nevertheless, there were lessons from the event.

We have since learnt we were victims of a third-party appliance 'zero-day' vulnerability in our co-lo VPN hosted at One Wiltshire where 280 ISPs connect. Many businesses and US government agencies were affected too.

As a TPN and studio assessed facility, we had done everything right, but things move fast on the dark web. In the end we did not get extorted, we rebuilt our Burbank IT infrastructure and got back to business. We are fortunate to be a global business with more than one site, so we were able to limit the issues and continue to support our clients.

My advice to all businesses is treat cyber risk like you do fire safety and assume you're under constant threat from arson. Make sure you're properly insured, follow the MPA best practices, and be prepared. Finally, if you have one site or facility, it's worth connecting with your industry peers to partner on a 'what if' basis for business continuity.

FROZEN

Louisa Sutherland-Smith Still bedazzled by the first half of *Frozen, The Musical*, my phone was buzzing when I checked it in the interval. I saw that I had been inundated with missed calls and messages from halo. As my children dragged me to the ice cream stand, I made a call back to base - "there's been some suspicious activity, we believe someone has tried to access our network". I bought my kids as much ice cream as they could carry and caught up on the situation.

One of our ops had spotted an unusual file on a corporate workstation and immediately notified their manager who in turn swiftly escalated it to a Senior IT Engineer, exactly in line with our training protocols. The file was quickly identified as an attempt by an "outsider" to break into our servers and in less time than Elsa's first half costume change, our teams had already started working their way through our security procedures. Our Cyber Emergency Response Team (CERT) discovered the source was ransomware and whilst we knew our systems were safeguarded, the "what ifs" just didn't bear thinking about.

Halo suspended all operations that Friday afternoon - we turned off servers that hadn't been powered down in years. Our IT and Engineering team then worked around the clock for days; scanning and restoring every machine, device, system and network in the facility. Meanwhile my management team and I followed up with our insurance company and their specialist legal advisers who supported us throughout the weekend, preparing us for various outcomes should the situation escalate. Thankfully, it never did.

Nothing more than that initial file was found; no ransomware note, no damage, and most importantly, no content came close to being accessed as the file was only found on our corporate network which is completely separate from our production servers. There was certainly disruption to the business - we had to stay closed over the weekend and the following Monday - but there is no doubt we took the correct



Heart of Stone for Netflix, film lab by Cinelab

action. Whilst others might see it as an extreme response, our delivery partners' content security teams praised us for mitigating what may well have proved to be a very real and damaging threat.

CHRISTMAS INTERRUPTED

Nick Platt Because Picture Shop works with many of the leading studios across the world on some of the highest profile projects, our security is as robust as we can make it. We pay a significant amount and undertake the most stringent security protocols to be Tier Zero compliant. This includes regular hardware and software audits, regular training across the organisation and dedicated security teams. Our corporate and content servers and networks are kept completely separate for this very reason. This is a requirement for some studios, like Disney, but we universally apply this across all facilities globally.

If there is a moral to this story, it is that we take pride in being methodical, thorough and robust in our approach to security, that we have everything locked down... and yet despite that energy and investment, if there's a hardware issue it can still be exploited.

I got a call telling me the IT team had detected some unusual activity on our corporate network – and that there had been an attempt to access some encrypted files and a ransomware note had been found. We had established procedures and protocols and a detailed Disaster Recovery Plan and knew what we had to do. We immediately cut everything off: we pulled the plug on our servers globally, closed all our sites down and called our insurers who parachuted in a team of cyber experts.

Of course, you have a moment when you are unsure of how bad it might be and what information has been collected, but thankfully they didn't access or exfiltrate any content or anything of value. But it takes a fair amount of investigation to figure this out, in our case over almost a fortnight. Although there was no material damage, in some respects I'm glad it happened over the Christmas period as the business interruption was significant while we fully investigated the matter extensively. You have to scan every drive and every machine to be 100% sure there is no breach. It took a lot of work over the holiday period by our amazing team of engineers when I am sure they would have rather been at home watching the shows they'd helped create. It goes to show why we need to have such complex and robust security procedures and protocols to ensure our clients content is kept safe as cyber security attacks are on the rise and getting more sophisticated by the day.

BANANA REPUBLIC

Adrian Bull In 2010, I got a call at six in the morning from an SVP at Warner Bros. We were working on the dubbing masters for Harry Potter 7 and the first 36 minutes of the film had been leaked on the internet. The SVP's point was that we were the only company that had distributed that content. We were dealing with over 30 foreign language versions for international theatrical distribution and this was a week before release. The only people that content could have come from was either us, as the creators of these versions, or the facility in one of the territories that was working on a version.

At that time the territories were probably unaware that all versions were uniquely forensically watermarked. As soon as we had a copy of the leaked files, we ran the decryption processes on them. By 2.00pm we had identified the South American territory involved. By 4.00pm MPA had representatives visit the facility where it was subsequently confirmed that some employees had been responsible for the leak.

STAYING AHEAD OF THE GAME - MONITORING CYBER RISK

Rob Jones, executive chairman, head of media, technology and cyber, Nirvana (working with KYND who provide cyber risk technology support)

According to a Qualsys 2023 report, more than 26,000 Common Vulnerabilities and Exposures (CVEs) were disclosed in 2023, surpassing the 2022 figures by over 1,500. While these numbers may seem alarming, only 206 (or around 0.8%) of these vulnerabilities had weaponised exploit code available, which if used would be very likely to compromise the target system and presented a significant risk to businesses. With CISOs being increasingly inundated with security alerts and striving to remediate as much as they can, prioritising the patching of the 'organisation killer' vulnerabilities over the thousands of others that don't pose a genuine threat to the organisation is paramount.

The speed of this remediation is also key. Leveraging its continuous exposure monitoring capability and proprietary risk intelligence, KYND monitored 3,500 organisations and calculated the average time to patch a vulnerability was 72 days. In contrast, Qualsys calculated the average time to exploit these high-risk vulnerabilities was 44 days. The ability to cut out 'the noise' and patch the right vulnerabilities at the right time is integral for reducing the risk of successful cyber-attacks.

The same proactive approach must be applied to mitigating zero-day vulnerabilities, which are discovered by attackers but yet unknown to the vendor, posing significant threats as they lack available patches. It is often a race between cyber-criminals attempting to exploit the flaw and vendors rolling out a patch to address it. For organisations, leveraging continuous cyber risk profile monitoring along with advanced threat intelligence capability such as KYND's to stay a step ahead of threat actors, and promptly applying released updates can help reduce the exposure window, even when dealing with zero-day exploits.

WHAT NEXT?

Threats are taking ever changing forms. With the rise of AI-driven social engineering, ransomware-as-a-service, and supply chain attacks among many others as well as the use of technology generally, what's next? While cyber-attacks won't go away and continue to evolve, it's our responsibility to continuously educate ourselves, adapt to emerging threats, and advocate for proactive cyber risk management strategies to help organisations protect themselves against today's dynamic threat landscape.

BEST PRACTICE

Ed Bengoa At ITN Post, we're lucky to sit behind the ITN-wide cyber security measures, but we still have to have stringent protocols within our facility to avoid any breaches. These range from the basics, such as disabling USB ports in all our edit machines, to enforcing virus scanning on rushes transport drives. Educating our staff is key to safety, training is ongoing, and it's delivered online globally, or in person within post.

Within our remote working environment, we use multi-factor authentication, in transit and at rest encryption, which are all paramount in preventing a successful attack. We ensure all our third-party services abide by these protocols.

We keep operating systems and relevant software up to date, and each machine points towards the ITN-wide Windows Update server to roll out relevant security updates where possible.

Behind redundant Palo Alto Firewalls, each machine runs a sophisticated, low resource, anti-virus software which interrogates and reports back immediately to our Cyber Security and our MDR (manage, detection and response) team, should a threat arise.

Nick Long Our first TPN Assessment was completed on their portal for which we received our Blue Shield. We took our time as we were upgrading and building new infrastructure at the same time and wanted to build it all around the TPN requirements - a blank canvas guided by the framework of sorts. There are a lot of policy documents required, a lot of which we had written down already but other stuff was in our heads so it was a really good process to not only draw up new documents but also amend existing ones and put them into a uniform template and management system in order to make them available to relevant parties and also keep an audit of changes and review dates.

As well as paperwork there are lots of questions and requirements around physical hardware and buildings. For example, we totally overhauled our CCTV and started doing DBS checks on all staff to fall in line with the best practice guide. We also implemented a new staff security training scheme which involves regular testing to ensure our team continues to be vigilant against threats like social engineering.

Once we completed our Blue Shield certification, we were assigned an assessor from ISE, who was great. As it was our first time, he guided us through everything and helped us in some areas that we were not too sure about.



Heart of Stone for Netflix, film lab by Cinelab

It took two very long sessions with the assessor to complete the Gold Shield questionnaire, checking over our documentation, completing a full walk through of our building and secure machine rooms and showing examples of training to ensure what we had declared on the questionnaire was the case.

After the ISE completed their report, we were assigned Gold Shield status with a list of remediations which we completed within a couple of months. We found it a helpful process.

THE WEAKEST LINK

Tom Mitchell While we have a conversation about how we can be secure and look after production IP, it would be remiss not to look at the whole picture.

It's puzzling that studios establish organisations like the TPN to audit and vet vendors but not production companies. Vendors invest significant time, labour and resources into implementing secure systems. They also bear the cost of audits and membership fees, further demonstrating their commitment to security.

On the production side, individuals on set ensure that COVID-19 rules are implemented, sensitive material around nudity is managed

THE ROLE OF THE TPN GOLD SHIELD ASSESSOR

Charlie Evatt, director and principal consultant, Evatt Industries

A TPN 'Gold Shield' assessment is performed by a TPN accredited assessor and involves review of a service provider's security posture against the MPA Content Security Best Practices and their additional recommendations.

This is how I approach an assessment engagement, which I undertake in the UK and globally.

Once a company has selected me to assess, I 'accept' in the TPN online portal. This starts a clock ticking: 15 business days until the assessment needs to be submitted to the TPN.

Once accepted, I review the service provider's self-attestations within the 'Blue Shield' questionnaire and any supporting evidence which has been uploaded. I review the materials submitted to build a picture of the security approach and identify any potential topics of discussion.

The service provider and I will conduct sessions with their team for the main part of the assessment to occur. These are either physical and on-site, or remotely with secure video conferencing. We will discuss the Blue Shield responses, implementations of the best practices and evidence submitted to create a clear picture of the service provider's security status. The high-level domains being assessed are organisational security, physical security, and technical security.

The service provider's team and I may identify areas which require more evidence than that initially submitted. I will request this either at the time or to be submitted within an agreed deadline.

Once the appropriate level of evidence is collected, I write up the report. For each best practice and related recommendation, I assess whether it is fully met, partially met, not met, or not applicable. For each of these items I describe specifically which evidence justified my assessment.

If any of the best practices or additional recommendations are not fully met, I detail where remediations are required, at a suitable level of detail.

I write a report covering each of the 66 best practices and related recommendations and submit it the TPN portal. The TPN perform a quality control check before releasing the report to the service provider and content owners.

The service provider then fills in their remediation plan, after which the 'Gold Shield' certification is given.



The Lost Women Spies for World Media Rights, picture finishing by The Finish Line

While major studios usually manage production security well, this is not always true for production companies. They often lack an audit process, TPN certification, or accountability, making them the weakest link in the security chain.

correctly, and health and safety protocols are followed. However, no one is specifically assigned to look after the security of the production itself. This oversight results in insecure content delivery methods, such as shipping hard drives in jiffy bags. Security personnel leave footage unattended on set or unencrypted media ends up being handled by unvetted minimal-wage personnel. Media is managed in unlocked offices and unsecured locations within hotel rooms.

Zeb Chadfield Getting production teams on board with security is super important, but simply convincing them to do basic things like getting editors to run the current versions of NLEs so that updated OS versions and security patches can be installed, feels like an uphill struggle. For those of us in post production, pouring money into security is a must, but if the producers or editors see basic security steps as too much of a hassle, keeping their data safe becomes nearly impossible, regardless of auditing and certification. This kind of attitude not only makes our job tougher but also puts our reputation and livelihood on the line if a security breach were to take place due to exceptions that have been made.

Paul Hillier I would be keen to follow up with the production companies about cyber security and see how we can support them with some solutions to mitigate risk. From what's been described, it is on set freelancers who have short-term involvement in the project, that could be a weak link. The question is who is accountable for that security risk and at which stage.

WHO CARRIES THE COST?

Zeb Chadfield The legal and insurance side of this has turned out to be way more interesting than I thought it would. Hopefully, it shines a light on just how complex and costly this all is and helps producers understand why we need to stick to certain security measures and best practices. It might be a good idea to consider a security charge that makes sense for productions of different sizes or as a percentage of the post budget. Bringing something like this into effect when the market is already shaky is going to be tricky, but it's crucial for making most security measures viable and hopefully broadcasters can get behind that investment to protect their assets.

Nick Platt Whilst the industry landscape is facing uncertainty following the strikes and other factors, it's a difficult balance to prioritise the high cost of security, infrastructure and running costs. However, we must ensure we protect both ourselves as studios and the industry together against this increasing threat.

Symon Roue There is a significant cost to fulfilling TPN and security arrangements. It requires a full-time member of staff to cover security. For Tier Zero or Tier One projects, should we have a surcharge universally applied?

Adrian Bull From a production perspective on set, that does happen. For Tier Zero and Tier One and Tier Two classifications, they set a different price point for your services. But only in production. Not in post.

Charlotte Layton But in post if you introduce that kind of levy, it will just get taken from our bottom line. It would have to be something that sits separately from the post budget.

10 THINGS YOU MIGHT NOT KNOW ABOUT TPN

Terri Davies, president, Trusted Partner Network & Stephen Stewart, consultant (TPN UK and EMEA Ambassador)

1. All eight major studios are TPN Content Owner Members – Amazon Studios, Apple Studios, The Walt Disney Studios, Universal Studios, Netflix, Paramount Global, Sony Pictures, Warner Bros. Discovery - in addition to other global Content Owners such as BBC Studios and Multichoice.

2. The Motion Picture Association (MPA) Content Security Best Practices are updated and published annually using feedback received from service/application providers and TPN assessors. TPN also meets with the TPN content owner members to map studio controls and agree on final updates before publication.

3. The MPA Content Security Best Practices are mapped to NIST, ISO, AICPA and CSA. ISO 2013 and 2022 are also matched to the TPN questionnaire to pre-populate answers as appropriate.

4. The new TPN+ platform includes a short baseline section that scopes each site or application's TPN questionnaire to avoid redundant or non-applicable effort.

5. Any service or application provider can create a TPN+ account and complete the TPN questionnaire to understand which of the MPA Best Practices they have not fully implemented, with no obligation to pay for TPN membership.

6. The TPN Blue Shield is the prerequisite for Gold and must be updated annually. However, it may also be a final choice for service/application providers who are not working on sensitive or early-window content.

7. The TPN Gold Shield renewal process is now on a two-year cadence and is only awarded after a plan or update is provided for each remediation item.

8. The TPN+ Company Registry is searchable by company name, service, region and TPN Shield status.

9. The TPN+ Application Registry is searchable by company or application name, service type and availability of hardening guidelines – which are downloadable by TPN members and non-members.

10. TPN wants and needs your feedback to keep improving the programme. Get involved.

Please email support@ttpn.org or click the "need support" buttons on the website (www.ttpn.org) or in the TPN+ platform.

ONE BODY

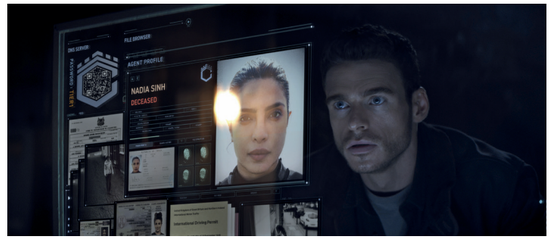
Charlotte Layton Collectively post vendors have always taken cyber security incredibly seriously and now more than ever, the threats are greater. It is important we have open dialogue with each other, as this is not an area any business should be trying to profiteer over another's misfortune. Racoon has a responsibility to our staff and clients to keep their data safe. Implementing rigorous security processes, protocols and applications is not a box ticking exercise for us. Continuing, regular and audited governance is essential. Training and empowering staff to understand how they need to remain vigilant is paramount. Ensuring we comply with industry standards, whilst 100% necessary, is onerous. Particularly for smaller businesses without dedicated security officers.

The notion of complying with one industry standard that all studios/streamers/broadcasters accepted at blanket level is appealing.

Adrian Bull I would love there to be one body that we could work with exclusively. When I first started this security journey back in 2007, it was the MPAA [now MPA] and the emphasis was on physical security. I welcomed the fact that the six studios had come together to manage the security risk requirements from a single governance perspective. Unfortunately, that never really happened, we still continued to have individual audits, just additionally now with the MPAA ones. When the TPN was created as a specific body to focus on security I hoped this would be finally solved. I didn't want to complete countless audits all with their own slightly nuanced requirements inevitably biased towards risks that they had individually suffered. To have one body to subscribe and work to makes much better sense. There's a time and labour cost to manage any security audit and that's a significant overhead for all our businesses to soak up.

It's not about annual or biannual audits because the security risks change constantly as technology evolves and with it come new threats. If you had one focussed body that would make me happy and the quality of reporting on potential security vulnerabilities could be better shared and better managed as well.

I immediately see a value from collaboratively bringing all parties together, particularly around cyber security, as our risks could be better understood and mitigated. I'm sure I'm not on my own. I would hope that a recognised industry body could additionally provide better understanding for insurers of our risks allowing for more appropriate support particularly if breaches do occur.



Citadel for Amazon Prime, digital imaging services by Cinelab

DEEPFAKE

Rob Jones CNN recently reported an incident involving a Hong Kong finance worker who paid out $25m following a video call with a deepfake CFO and other colleagues. The finance worker had been sent a suspicious phishing email from the UK-based CFO requesting a secret financial transaction. The strength of the video call where his colleagues looked and sounded as he remembered them was sufficient.

Cyber-crime is one of the biggest threats facing businesses today and the number of reported cyber-crimes has increased dramatically since 2017. Most cyber-attacks are not directed at a specific company but by cyber-criminals trawling the web for technology vulnerabilities, particularly those found in cloud-facing hardware and software. Although vendors look to stay ahead of exposed vulnerabilities by releasing patches, the speed to action them is often slower than the speed with which cyber-criminals exploit them.

Find out more at ncsc.gov.uk and talk to your insurance provider and TPN.

TYSERS LIVE CYBER SECURITY RECOMMENDATIONS

Toby Clowes, director and head of cyber

1. Recognition of cyber risk from the board level down. The threat is no longer the sole responsibility of IT. It requires a company-wide approach.

2. Continued Investment in IT infrastructure and security measures. The risk profile is one of constant evolution and today's protections can be tomorrow's weaknesses.

3. An understanding of where/what assets of value are held at any one time. Whilst some of these may be cloud hosted, ultimate responsibility falls back to the data collector or those entrusted first-hand with its safety. Whilst fault may lie with a third party, what protections does a post house/entity have under such contracts?

4. A comprehensive Business Continuity Plan and Disaster Recovery Plan. Do the respective members of a firm know how to react in the event of a cyber-attack? Insurers would expect both these measures to be in place and tested at least every 12 months.

5. Multi Factor Authentication (MFA) is deemed as a key measure in preventing ransomware events. Have it in place on all assets where possible.

6. Limit the number of privileged accounts and ensure additional protections around their access.

7. Deployment of next generation endpoint monitoring and isolation tools. Catch the event early and isolate it.

8. Isolation of end-of-life operating technology and software. Where software is no longer supported, look to segregate these systems away from outward (internet facing) infrastructure.

9. Air gapping and segregation – whilst not always practical for all business, look to segregate systems from one another.

10. Train, train and train your employees. A business can have the best security available but the workforce is the most likely weakness in any entity. Phishing training and cyber awareness are proven to reduce the chances of a successful attack.

11. Look to cyber insurance as a final balance sheet protection but know how to activate it fast. It's not a replacement for good cyber hygiene but can be instrumental in a quick and cost-effective recovery. Insurers are well versed in how to handle an incident (they've had more practice) and can calmly recommend a best course of action.