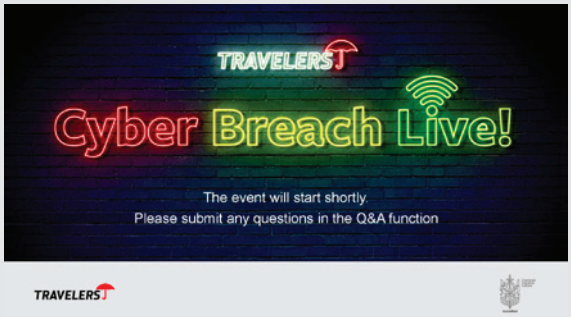
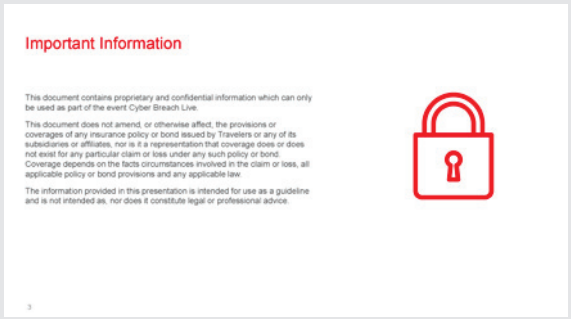
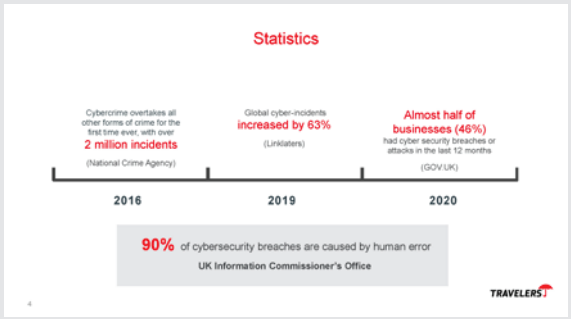
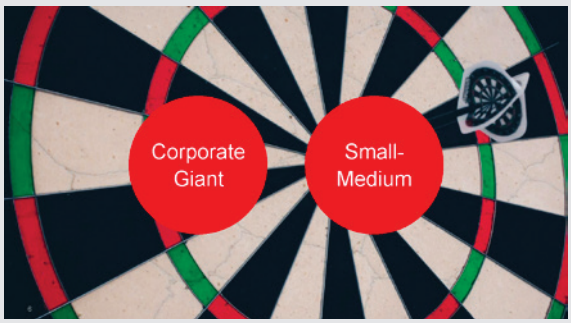
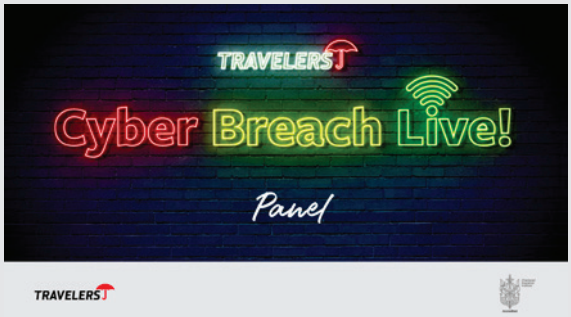
TRAVELERS

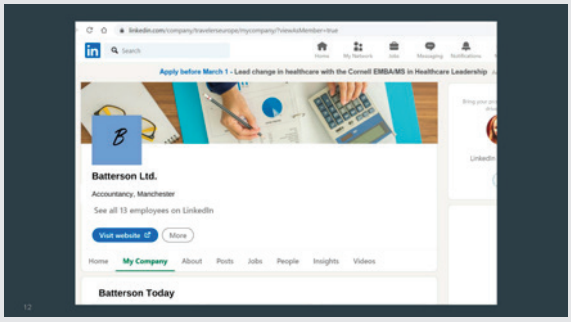
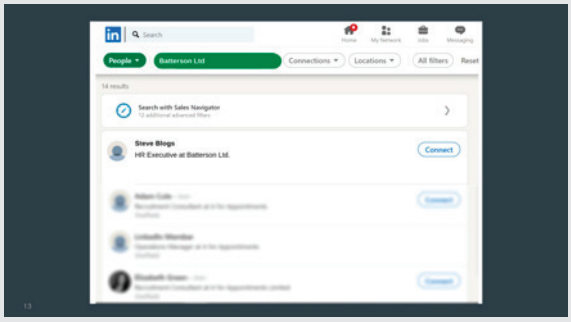
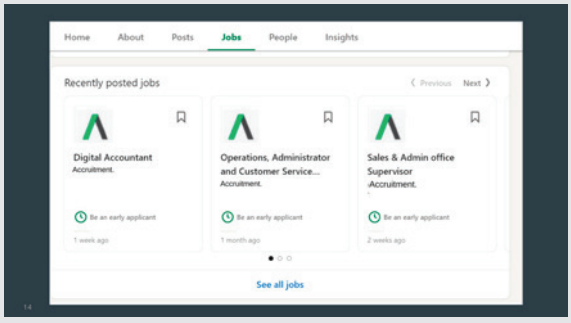
DIY script

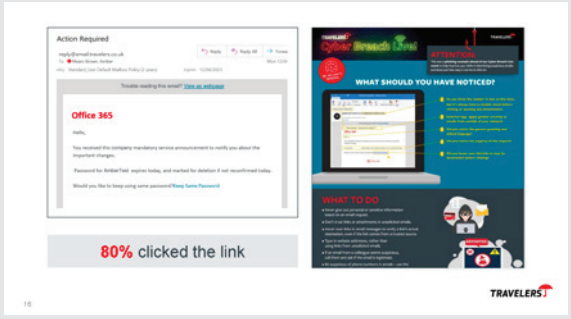
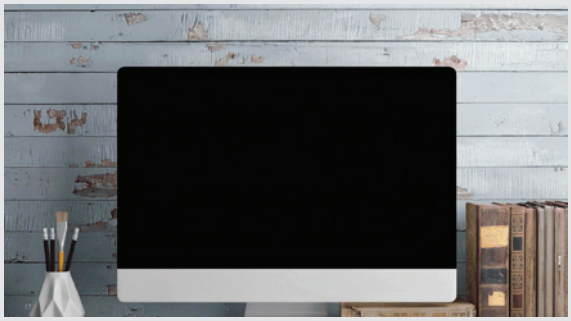
Slide	Script
 **Slide 1** (1 min) **Holding slide whilst audience log in**	None required
 **Slide 2** (30 secs) **Welcome and intro to event**	**Host:** Hi everyone and thank you for joining Cyber Breach Live. I'll be your host for the event. – We have recordings from 3 cyber experts from the original event: – **Davis Kessler**, the Head of Cyber Underwriting at Travelers – **Tom Pelham**, a partner at Kennedy's Law – **David Wiggett**, Associate Director at KIVU Consulting
 **Slide 3** (30 secs) **Legal disclaimer**	**Host:** Before we begin our exercise, I have been asked by the Legal team at Travelers to remind you all that this is a work of pure fiction. Whilst we do reference some actual individuals and events – they are purely for illustrative purposes only. The other names, characters, businesses, places, events, locales, and incidents are either the products of the author's imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental. You can all be secure in the knowledge that you will survive this attack unscathed.

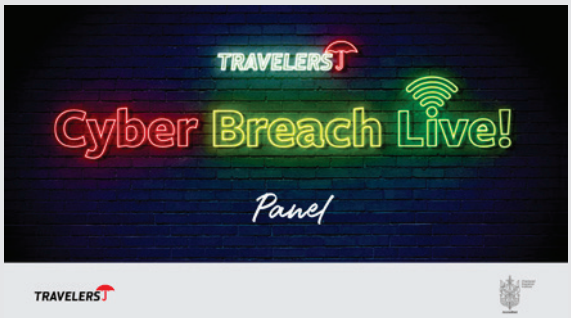
Slide	Script
 **Slide 4** (3 mins) **Some stats**	**Host:** In 2016, the UK's National Crime Agency found that cybercrime had overtaken all other forms of crime for the first time ever, with over two million incidents recorded in that year. A report by Linklaters in January 2019 stated that global cyber-incidents increased by 63% since 2016. In a 2020 Government survey, almost half of businesses (46%) had cyber security breaches or attacks in the last 12 months. Cyber-attacks are also becoming more sophisticated and varying in delivery. However, they overwhelmingly share one thing in common: According to the ICO and Cybint, over 90% of cybersecurity breaches are caused by human error.
 **Slide 5** (30 secs) **Setting up the scenario**	**Host:** To make this experience as realistic as possible, we're going to ask each of you to take on some new roles over the next hour. Firstly, we want you to assume the role of an **attacker**.
 **Slide 6** (30 secs) **Dartboard image**	**Host:** You've got a new ransomware code from the Dark Web and you're looking for your next target... **POLL LAUNCHES**

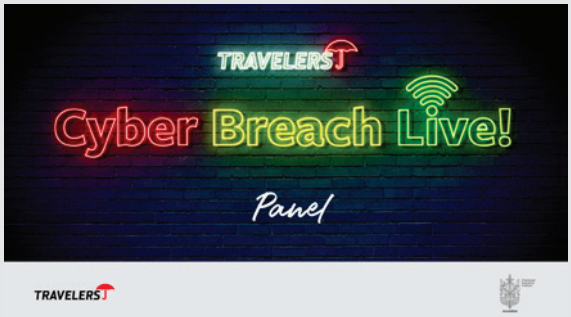
Slide	Script
 **Slide 7** (30 secs) **POLL**	**Host reads out options:** Which would you go for? – Big Corporations have money, but a lot of security and shareholders – Smaller companies offer a potentially easy win, with less security in place and minimal employee training
 **Slide 8** (3 mins) **Stats**	**Host once poll has closed:** An increasing number of attackers would go for Batterson Ltd; around 43% of cyber-attacks targeted small businesses in 2019 (Verizon 2019 Data Breach Investigations Report), up from 18% in prior years. – Smaller organizations (1–250 employees) have the highest targeted malicious email rate at 1 in 323. (Symantec) – £8,170: average annual cost to SMEs that lost data due to a breach (Gov.uk, 2021) – 43% of SMEs have no cybersecurity defence plan in place (Cision PR Web 2020) 66% of senior decision-makers at SMBs do not believe they are likely to be targeted and 60% report that they do not have a cyber-attack prevention plan (Keeper, 2019) We also see a lot of indiscriminate attacks – attackers don't know or seem to care who they target, and it's become more of a numbers game than a targeted approach. What does this mean? Malicious software scans for any vulnerabilities and goes for anything that has an opening. Smaller businesses are more likely to have vulnerabilities; therefore, they are more likely to be hit. Whichever way you look at it, SMEs are at high risk of an attack.

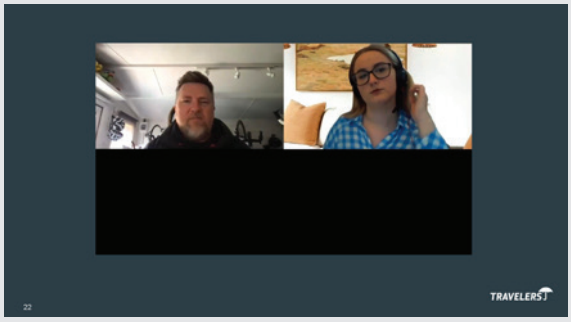
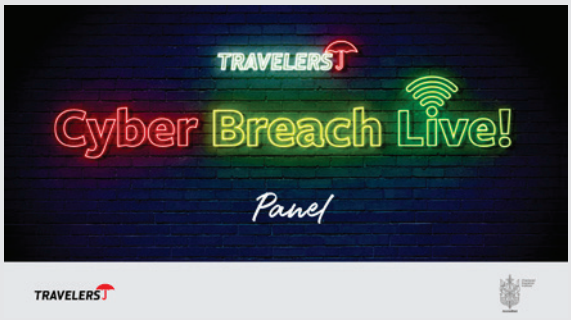
Slide	Script
 **Slide 9** (2 mins) **Panel**	**Host:** Let's go to our experts, what trends are you seeing in the insurance market for SMEs? **Video:** SME Insurance Trends 1 – Davis Kessler **Host:** There's an interesting quote that 'If you want your senior management to care about incident response, burn down the office across the road'. And that seems to apply to cyber events as well. Do you see that a lot with small businesses? Do they take things more seriously if they see a peer or similar company hit? **Video:** SME Insurance Trends 2 – Davis Kessler
 **Slide 10** (30 secs) **Research**	Okay, so you've decided to target Batterson with an attack. Time to do some research! Where could you find information to help your hack? **POLL LAUNCHES** **Host to read out the options:** – Company website – LinkedIn – Calling the company – Visiting the office – Google – Dark Web **ONCE POLL HAS CLOSED:** The answer is, scarily, any and all these avenues can be useful to an attacker!
 **Slide 11** (3 mins)	**Host:** Let's go to our panel for comment. David over to you: **Video:** Information gathering – David Wiggett **Host:** It's really interesting, that in most cases human error is the root cause. For example, NASA say that we can improve our technology and constantly update software, but the human hardware will always be a limitation for space travel. In the same way with cyber-attacks, we are all fallible and likely to fall for a phishing attempt or social engineering ruse at some point.

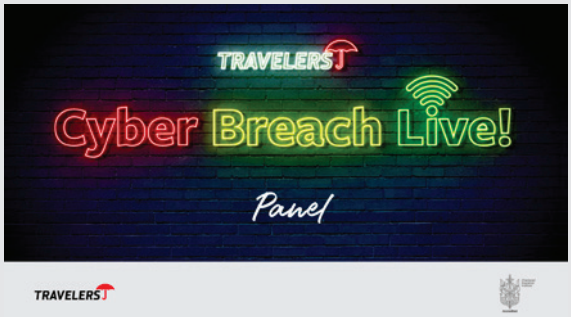
Slide	Script
 **Slide 12** (click through quickly) **Batterson Company profile**	**Host:** A simple way that attackers can find information is through social media and company websites.
 **Slide 13** (click through quickly) **Steve who works there**	**Host:** You've identified Steve from the HR department at Batterson, and know they use a recruitment firm for potential new hires.
 **Slide 14** (click through quickly) **Recruitment**	**Host:** You've found a way in.

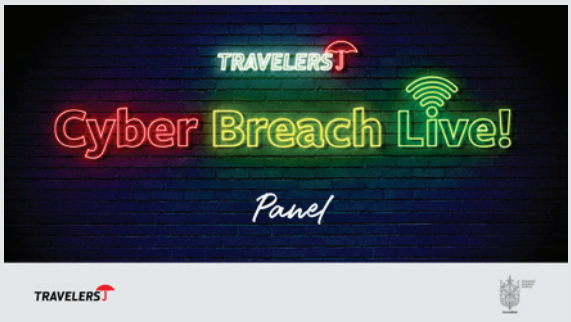
Slide	Script
 **Slide 15** (30 secs) **Phone call audio**	**AUDIO CLIP** **HOST (AFTER AUDIO HAS PLAYED):** And it's that easy!
 **Slide 16** (1 min) **Phishing example**	**Host:** At the original event, the organisers sent a phishing example to those who registered, to demonstrate just how simple an attempt can be. Over 80% of those who opened the email then clicked the link. I'll let that sink in... But back to our scenario: You are now the Head of IT at Batterson Ltd. It is 08.30 on a Tuesday morning and you have just made a coffee. You log onto the network and...
 **Slide 17** (30 secs) **There has been an attack (animated popup)**	**Host:** The network has been hacked and it looks like a form of ransomware has entered the system, locking you out.

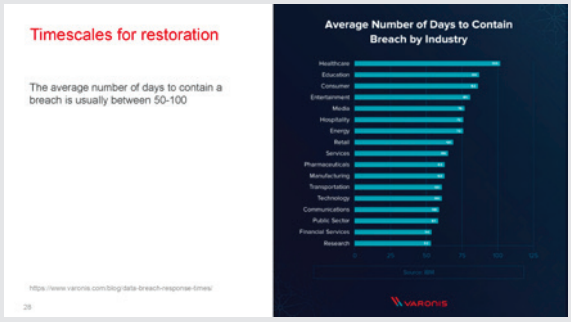
Slide	Script
 **Slide 18** 14.19 – 14.20 (1 min) **You've been hacked**	**POLL LAUNCHES** **Host:** What do you do next? **Host reads out options:** **A.** Notify the Information Commissioner's Office (ICO) that there has been a personal data breach **B.** Contact Action Fraud or the police **C.** Contact your insurer and advise them of the situation **D.** It's clearly a prank - hope it all goes away **ONCE POLL HAS CLOSED:** Hopefully you all agreed that the most appropriate next steps are to contact your insurer and advise them of the situation. It is important that, as part of a leadership team, you are aware of what the appropriate course of action is at this juncture and understand how your cyber insurance policy works, as not all of them are the same.
 **Slide 19** (3 mins) **Panel**	**Host:** Let's hear what our experts have to say on this matter. Tom and Davis over to you. **Video:** Dedicated Cyber & access to specialists – Davis Kessler **Video:** Breach Coach Importance – Tom Pelham **Host:** It's about being transparent in a controlled way. Walking that fine line between being up front, but also avoiding highlighting weakness, and having expert advice can really help with that.

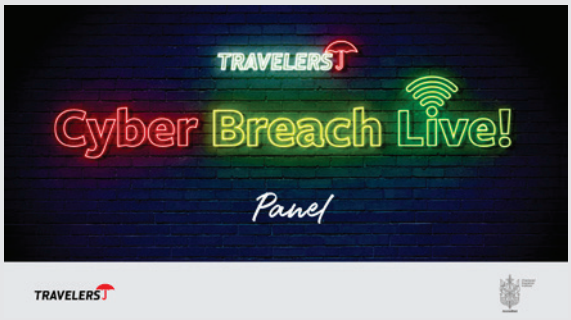
Slide	Script
 **Slide 20** (1 min) **POLL**	**Host:** So, having spoken with your insurer, they have advised that the next appropriate course of action is to gather as much information as possible around what has happened. If you realise that data has been compromised, as part of your breach response process you will need to start notifying the right people at the right time. **POLL LAUNCHES** **Host reads out options:** **A.** All existing customers **B.** Suppliers **C.** Breach coach **D.** Press **E.** Staff **Answer:** The correct answer is Breach Coach **Host:** There will be many people you do eventually need to inform, but you need to ensure you manage these communications effectively to avoid creating more problems. When breaches happen, a comms mistake can be catastrophic, and your legal breach coach can help with that.
 **Slide 21** (6 mins) **Panel**	**Host:** Let's go to our panel on why managing the message is so important **Video:** Managing the message 1 – Tom Pelham **Video:** Managing the message 2 – David Wiggett

Slide	Script
 **Slide 22** (3 mins) **Breach triage call**	**Host:** Okay, so back to our scenario. Your insurer has set up a triage call between yourselves at Batterson, your assigned legal breach coach and a claim specialist. **Video:** Triage Call
 **Slide 23** (6 mins) **Panel**	**Host:** There is no time to sit back and relax now that your insurer and legal breach coach have been appraised of the full situation at your end. With all the facts at hand, your breach coach will immediately get on with advising and remediating as much as possible in the next few days. They have given you instructions and will now start building a dedicated team of vendors to respond quickly and effectively to your cyber incident. Internally you've done a stellar job so far, but this isn't always the case. What could have happened if Batterson had 'gone it alone'? **Video:** Going it alone 1 – Tom Pelham **Video:** Going it alone 2 - David Wiggett

Slide	Script
 **Slide 24** (1 min) **Forensic investigators**	**Host:** So, you can see independent third-party partners with specific expertise can really help. You know from your conversation with your Breach Coach that the priority now is to engage a Forensic Investigator. **POLL LAUNCHES** But what does that actually mean and how can they help? **Host reads out options:** **A.** Ability to advise C-Suite on who attacking groups are and likely chain of events **B.** Associated timescales for different ransomware groups **C.** Incident Response **D.** Digital Forensics **E.** Restoration following business interruption **ONCE POLL HAS CLOSED** **Host:** the answer is all of the above. Let's hear from our experts around what this service does and how they can help you out in this particular situation.
 **Slide 25** (2 mins) **Panel**	**Video:** Forensic Investigator role 1 - David Wiggett, Forensic Investigator role 2 – David Wiggett **Host:** Your insurer and breach coach have arranged for these services to be engaged, and with their experience of a wide range of cyber-attacks, they are soon able to identify the kind of ransomware attack you've experienced.

Slide	Script
 **Slide 26** (1 min) **Next steps**	**Host:** As the investigation continues, it confirms your fears by identifying that data has been stolen from your system via this back door - you are dealing with a full-on data breach. You are advised that customers contact details including names, email addresses and invoicing details have been stolen, along with associated payment data including credit card information. **POLL LAUNCHES** Once you realise this, what should you do? **Host reads out options:** **A.** Notify the Action Fraud of data theft **B.** Notify the ICO of a personal data breach **C.** Email all of your customers that their data may have been compromised **D.** Put a post on social media admitting to a breach occurring **ONCE POLL HAS CLOSED** **Host:** Notification of the ICO would need to happen alongside the investigations into the incident. Any notifications would also always be subject to the legal advice from your Breach Coach.
 **Slide 27** (6 mins) **Panel**	**Host:** Our panel can tell us a bit more about the ICO, what and when they need to be told, and the importance of discussing communications with your Breach Coach **Video:** ICO and Official notification – Davis Kessler **Video:** ICO: What not to do – Tom Pelham

Slide	Script
 **Slide 28** (4 mins) **Restoring timescales**	**Host:** As well as notifying people, you'll need to take action now to remove the malware from your systems and take steps to mitigate this risk for future. How long might this take? **Video:** Restoring systems: How long will it take & what skillsets are needed? – David Wiggett
 **Slide 29** (30 secs) **POLL**  **Slide 30** (30 secs)	**Host:** Now, all of this work is going to cost a fair amount. So, when it comes to insurance, which policy do you think Batterson was likely to have? **POLL LAUNCHES** **Host reads out options:** **A.** Standalone **B.** Packaged bolt-on **C.** Basic **D.** None at all **ONCE POLL HAS CLOSED** **Host:** They are likely to have hadnothing at all or, at best, a 'Packaged' bolt-on policy.

Slide	Script
 **Slide 31** (1 min) **Costs**	**Host:** So, if you were in that 40% without insurance (Travelers, 2020), this scenario could have had a starting cost of over £130k, not counting the business downtime and lost income you would experience. This kind of cost we can all agree could make or break an SME like Batterson Ltd.
 **Slide 32** (6-8 mins) **Panel**	**Video:** The cost of a breach: Insurance – Davis Kessler **Video:** The cost of a breach: Long-tail liability – Tom Pelham **Video:** The cost of a breach: Ransomware trends – David Wiggett
 **Slide 33** (1 min)	**Host:** Thanks to the help of your IT team, your insurer, legal breach coaches, and all of the 3rd party vendors, it would seem the situation is coming under control. Well done, you and Batterson for having survived a cyber breach! Although there is no such thing as a good cyber breach, by acting quickly and engaging all the right people, your reputation is intact, and you live to fight another day.

Slide	Script
 **Slide 34** (8 mins) **Panel**	**Host:** Onto our last panel discussion of the session. After experiencing a cyber incident like this, there will be many questions still left to answer, but the most important one is how do you make sure this doesn't happen again? What do you need to consider moving forwards as part of your cyber risk prevention process? How can insurance help? What would experts recommend a business like this to consider? **Video:** Mitigate future risk – David Wiggett **Video:** Mitigate future risk – Tom Pelham **Video:** Mitigate future risk – Davis Kessler
 **Slide 35** **Thanks for joining**	**Host:** As this session has demonstrated, it is important to investigate anything that looks suspicious. If it turns out to be nothing then at least you are able to test your breach protocols, but if it is a breach then you have more chance of stopping serious damage. Now is the time to take the right steps to ensure you are protected. Cyber risks are evolving and changing on a frequent basis, with new threats emerging every day, so the cover and protection needed has to be considered seriously. Thank you.

Useful Resources:

https://logsentinel.com/blog/2020-data-breach-statistics/?cookie-state-change=16134731497O5
https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html
https://www.cpomagazine.com/cyber-security/smb-study-reveals-majority-of-small-businesses-arent-taking-cyber-attacks-seriously/
https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/
https://www.purecloudsolutions.co.uk/ransomware-statistics-cyber-threats-in-numbers/
https://spectruminternet.com/news-views/10-shocking-ransomware-stats-for-businesses/
https://heimdalsecurity.com/blog/ransomware-payouts-of-2020/
https://serbusgroup.com/comms-posts/ransomware-in-2020-uk-and-global-threat-overview/
https://eriskhub.com/mini-calc-usli

Speaker bios for Cyber Breach Live

Panellists

Davis Kessler
Head of Cyber, Travelers Europe

Following five years' private legal practice, Davis Kessler joined the Travelers product development team in the US in 2012, and quickly began focusing on cyber coverage issues. In 2018 he transitioned to Travelers Europe to develop the company's standalone cyber proposition. Davis has led the cyber underwriting team since launching that product in May 2018.

Tom Pelham
Partner, Kennedy's

Tom is a partner specialising in cyber, breach response and data risk and he leads the firm's global Cyber and Data Risk practice. Tom has extensive experience in advising on the management and containment of data breaches and the regulatory issues flowing from them. He has acted on some of the world's most high-profile breaches as well as a huge variety of domestic cyber incidents involving ransomware, data exfiltration and system compromises. He has been instrumental in developing the firm's global cyber team and is regularly instructed to advise on the EU implications of breaches in the US, Canada and APAC.

In additional to his breach response practice, Tom advises on data protection issues and the defence of regulatory proceedings brought by the ICO. He is also one of the leading figures in the emerging field of data subject claims and has assisted countless clients in developing defence strategies against claims brought by those seeking redress following data breaches.

Tom is widely known as a co-host of Kennedys' Cyber Sounds podcast and as a regular speaker at events across the globe. He is a member of the IUA Cyber Claims Committee and the FOIL Cyber and Digital Liabilities Sector Focus Group.

David Wiggett
Associate Director at Kivu Consulting

David Wiggett is an Associate Director at Kivu Consulting, an international technology firm specializing in the forensic response to data breaches and proactive IT security compliance and risk reduction. David leads Kivu's UK and EU Incident Response and Post Breach Remediation team based in London, and has supervised cases globally involving public entities, major corporations in manufacturing, financial services, professional services and healthcare, and non-profits. David has particular expertise advising boards and senior management on responding to cyber extortion, explaining risks, technical constraints and possible outcomes in clear terms. He has worked with most of major insurance carriers and UK law firms handling cyber incidents and has provided an interface between clients and law enforcement.

Prior to joining Kivu, David spent 20 years in the West Midlands Police, including six years in the West Midlands Regional Organised Cyber Crime Unit, where he planned and implemented a range of technical solutions while conducting in-depth investigations within the Regional unit. He presented evidence to various bodies including the Crown Prosecution Service, Crown Court and Europol whilst working on international cross boarder investigations. David has testified in the Crown Court and Magistrates' courts.

About Kivu: With offices in the US, London and Amsterdam, Kivu is a pre-approved cyber forensics vendor for all leading North American and European cyber insurers. Kivu handles the technical response and remediation in network intrusions, phishing attacks, ransomware incidents, and accidental exposure of confidential information. Kivu also offers pre-emptive services including risk assessments, gap analysis, pen testing, and tabletop exercises. Kivu incorporates intelligence from its incident response cases to prepare against current attack vectors and implement best practices in security defenses. Kivu has pioneered an incident response protocol of remote analysis and data collection, allowing Kivu's analysts to immediately commence work anywhere in the world without the need of attending onsite, and is the acknowledged industry leader in the response to cyber extortion and ransomware.

Travelers Contacts

Cyber Team

Davis Kessler
Head of Cyber Underwriting
dkessler@travelers.com
+44 (0)20 3207 6571

Lisa Farr
Cyber Development Underwriter
lfarr@travelers.com
+44 (0)20 3207 6567

Regional Distribution Team

James Fone
London & South East
jfone@travelers.com

Jon Ashton
London & South East
jashton@travelers.com

Ciaran Simms
South West & Wales
csimms@travelers.com

Kiran Newey-Jones
Birmingham
kjonesne@travelers.com

Nicki Kelly
Manchester
nlkelly@travelers.com

Ian Robinson
Leeds
irobins2@travelers.com

Francesca Kelly
Dublin
fkelly2@travelers.com

Carolyn Conlan
Dublin
cconlan@travelers.com

Gerard McLaughlin
Dublin
gmclaugh@travelers.com

Travelers operates through several underwriting entities through the UK and across Europe.
Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk **travelers.ie**