Tracking the genesis of cybercrime

Delivering the keynote speech for Aon's *Live Webinar: Mitigating Risk through Cyber Insurance on the 10 March, 2021*, investigative journalist Geoff White traced the genesis of today's cybercrime – pointing the finger at three suspects – and what it means for the evolving cyber risk for businesses.

Contact Information

Mark Brannigan
UK Head of Cyber Solutions
Cyber Solutions
mark.brannigan@aon.co.uk

"Why has cybercrime become the massive risk we're seeing today?" asked investigative journalist Geoff White, addressing Aon's Live Webinar delegates. "It's not just because we're all using computers. There has been a shift in the dynamics behind cybercrime over the last ten years... because three key areas have come together."

Those areas are can be represented by three prominent names in the world of cybercrime – Jake Davis, Evgeniy Mikhailovich Bogachev and Park Jin-Hyok – who, according to White, have all played a part in weaving together three different strands of cybercrime to transform the cyber threat and risk for organisations and businesses around the world.

Manipulating the media

Take Jake Davis first; as a hacktivist and key member of black hat computer hacking group LulzSec, he helped move hacking on in terms of media exposure. "They understood how the media works and how to use that to make their hacks more impactful," said White, explaining how the group once broke into the content management system for the Sun newspaper's website, changing the lead story to report the (false) death of the newspaper's owner Rupert Murdoch.

Turning to Russian hacker Evgeniy Mikhailovich Bogachev who was behind the most profitable banking Trojan virus ever created. "[Bogachev] brought Silicon Valley tactics to cybercrime. He created the Microsoft Windows of cybercrime," said White, who described the sophisticated, organised crime operations behind the Zeus banking Trojan. And thirdly, White described North Korea's elite and well-funded state-sponsored hackers – Lazarus Group, represented by Jin-Hyok. "Lazarus was reportedly responsible for the Sony hack in 2014 and WannaCry attack in 2017."

Swapped tactics and techniques

The methods of hacktivists, organised crime and state sponsored actors have effectively merged said White. "They've swapped tactics and techniques which is what has made them so much more dangerous...and is causing greater problems for organisations." To evidence the claim, White detailed the 2018 cyber attack on India's Cosmos Bank which showed links between state-sponsored actors and organised crime.

Bank raid

It's believed that Lazarus carried out a complex raid on Cosmos that involved compromising the bank's ATM system, managing to extract US$11 million over 12,000 transactions in just a two-hour period. The challenge for Lazarus, was how to get the money back from the individuals they'd used to extract the money at the ATMs, to which the answer must have been organised crime groups, said White. "Clearly there are linkages between the state-sponsored hackers and organised crime networks. The only way of enforcing a criminal enterprise is through violence or the threat of violence...there must be linkage with organised crime."

Impact on businesses

What does this all mean for businesses? "We are now in a situation where we're getting a collapsing together of nation state government hackers, with organised crime elements, and with hacktivists/low level media manipulators," cautioned White. "As these three groups learn together and swap tactics, it becomes more difficult to work out where the threat is coming from.

Take the SolarWinds incident where nation state hackers – believed to be from Russia – used organised cybercrime tactics to hit as many organisations as possible in a 'spray and pray approach' to get access. "That is straight out of the playbook of the organised crime gangs. You are now as likely to be hit by a nation state actor regardless of whether you thought they were the threat or not, so calculating where your threat comes from gets much harder," said White.

The other consequence of these three groups merging their methods is for your risk, said White. "In previous days you could work out what the risk is if you were hacked. A hacktivist group would go to the media, while an organised cybercrime gang probably wouldn't go public. But because of the collapsing together of the tactics of these three groups, you're now seeing organised crime gangs learning from hacktivists and affecting how that risk will play out."

Ransomware evolves

This trend is particularly evident in ransomware. Previously groups would break into an organisation, encrypt their files and demand a ransom but they'd stay silent said White. "But these tactics have shifted. Ransomware groups will break into an organisation, steal sensitive information, then drop the ransomware and say 'unless you pay this ransom, we will leak this sensitive information'. Organised crime gangs have learnt how to use the media and public exposure and use reputational damage to get more bang for their buck. If and when your cyber attack happens, it gets harder and harder to work out what the risks might be going forward."

Cyber cover: an insurer perspective

An insurer panel discussion – chaired by investigative technology journalist Geoff White during Aon's Live Webinar: Mitigating Risk through Cyber Insurance on the 10 March 2021 – featured Nicholas Nemetz from Chubb's Cyber and Technology Practice and Mike Tewfik from Beazley. The discussion ranged from talk about the increase in ransomware, how businesses can better protect themselves, and how cyber insurers are reacting to the changing cyber threat.

AON

Q: What is the scale of the ransomware problem?

Mike Tewfik: "Cyber criminals still look to the path of least resistance. The model is quite simple which might be phishing, sending malicious links and attachments, but also what we're increasingly seeing is access through open or unsecured ports – the equivalent of leaving your front door open. We're also aware of a few incidents that the criminals had actively looked for cyber insurance documents once they gained access to see how much cover a business has before requesting a ransom."

Q: What is the process of settling a claim for a business hit by ransomware?

MT: Invariably you'll have legal advice, IT forensics, and an experienced cyber negotiator [involved] – they all play a vital role. The process can be as short as one or two weeks, but ultimately what they're doing is buying time and seeing whether you don't have to pay the ransom – do you have viable backups for example?"

Q: Is ransomware predominantly a US issue?

MT: The US has been targeted more by cyber criminals. For 2020, there was a 40% increase in ransomware attacks globally, but in the US that figure was 140%. But we're seeing ransomware increasingly in Europe, UK, Asia and South America. We're also seeing more SMEs and smaller middle market businesses hit as well as listed entities."

Q: What steps does an insurer go through before paying the ransom?

MT: "In the US, the model tends to be to pay the ransom. The business controls particularly in the middle market aren't as good in terms of back-ups so they often don't have a choice but to pay. Ultimately, it's the client's choice; insurers will not make that decision.

Q: In view of the recent Microsoft Exchange incident and the number of victims involved, is there a danger that cyber could become an uninsurable risk?

MT: "The insurance industry is looking closely at this type of aggregated risk and exposure. It's very real. Most businesses are moving to the cloud and there are three main suppliers – what if they get hit? We're looking to manage the exposure and ensure there is longevity in the insurance product."

NN: "The insurance industry can manage some of that volatility through changing terms and conditions, managing capacity, increasing rates, and increasing deductibles. All these changes go towards creating a more sustainable market into the future."

Q: What are the key security indicators underwriters want to see before accepting a risk?

MT: "We look for fundamentals such as the easiest route in, which at the moment is open and unsecured ports. We look at end of life exposure as well, so are those unsupported systems managed? Are they segregated from the rest of the network? We also look at basic things like mandatory employee training – including for those in the C-suite – and multi-factor authentication."

Q: Do cyber insurers have flexibility on the security requirements for smaller businesses?

NN: "Cyber is a business risk that needs to be raised up the priorities of many organisations. But not everything needs to be expensive. It's more of an enterprise approach: here's our risk, here's how we manage and minimise it. A lot of that can be done with simple tools. The willingness to share information with insurers is also very helpful and shows a commitment to cyber security."

"It's often educational for the clients to understand what underwriters are looking for so they can change their priorities or amend their roadmap for cyber security. Going through a longer proposal form highlights areas and tasks for companies to take on in order to improve their risk."

Q: Do organisations practise the recovery of their systems after a cyber-attack?

MT: "Probably not enough. Businesses say they back-up systems and say they have appropriate segregation, but if you haven't tested the restoration of that critical data then you don't know, in a live situation, how long it will take you. It's often not a quick fix."

AON

Q: Are we seeing more willingness and openness to share experiences from cybercrime?

NN: "It's improved and a lot of the notification requirements have improved that transparency. Chubb has a publicly available claims website that has a database of all the claims we've see in the past 15 years. That's one way we're helping to contribute to that information sharing."

Q: Has there been an increase in people falling victim to phishing emails now they're working from home and has the insurance market adapted its policy cover?

NN: "In general, the number of COVID-19 related phishing incidents has increased significantly especially in the early days of the pandemic. It's important for companies to educate their employees on what those threats are. Remote working is increasing exposure, but awareness has improved partially because employers are willing to educate employees."

MT: "As the threat changes, the cyber insurance market has to change to stay relevant."

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Aon UK Limited
Registered in England & Wales No. 4396810
Registered office: The Aon Centre | The Leadenhall Building | 122 Leadenhall Street | London | EC3V 4AN