CMS Funds Group

Don't be the weakest link | Managing data and cyber risk

Risk, Resilience and Reputation Webinar Series

*The webinar in our **Focus on Funds | Risk, Resilience and Reputation** series saw CMS partners Chris Luck, Emma Burnett, Tom de Cordier, Lee Gluyas and Amit Tyagi discuss the implications of data management and cybercrime. The full recording is available here.*

Just about every business is a technology business.

And just about every business faces questions of data management and challenges of cybercrime. In the UK, the annual cost of cybercrime is estimated £27bn[1]. Globally, this figure was recently placed as high as €530bn[2].

Cyber criminals are relentless and sophisticated. But there are numerous ways to foil such activity – such as the simple use of multi factor authentication – and an array of options to minimise or recover from successful attacks – from insurance to free tools from CMS, linked at the end of this article.

Multiple avenues of attack

Given cybercriminals change and adapt quickly, it is worth identifying the sort of business threats that CMS and other experts regularly observe in the UK and EU. They are varied but often fall into one of four camps and are equally relevant to Funds.

Double extortion attacks are the theft of data – known as exfiltration – accompanied with a ransom demand, usually in a virtual currency. A failure to pay is likely to result in stolen data

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

2 https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

appearing on a doxing site (cyber industry jargon, derived from “dropping documents or docs”). These attacks are the lion’s share of incidents that pass across our desks.

A permutation of the above is an advanced persistent threat: or a state-sponsored hack plus exfiltration of intellectual property, often for espionage rather than commercial gain. A defence industry client was subject to such an attack recently in an incident focused on sensitive data.

A ‘person in the middle attack’ sees a senior staff member’s mailbox hacked – often for financial gain. For example, UK and European businesses and Funds send millions of payment requests each working day. Criminals intercept a request, change the bank account details, receive the money, and then transfer it rapidly to a difficult-to-access location. Regrettably, these are common and lucrative for the criminals.

We sometimes also see disgruntled workers undertaking similar hacks – not to extract money but rather to embarrass a company, Fund and their managers, steal confidential information or inflict comparable, non-financial damage on it. These are rarer but still damaging.

Multiple blocking and coping mechanisms

There is one thing we always recommend when working with clients: call your insurer’s or your broker’s hotline.

All insurers have a rapid response number, and we advise people to use it, even if they’re unsure if they have been attacked. People should also call even if they are unsure about policy coverage because talking the issue through with an expert may identify coverage opportunities.

At the same time, be careful about disclosing too much information. It is a prerequisite to discuss the issue in depth with your insurer – but just about every other party or stakeholder should be treated on a need-to-know basis.

Legal counsel should be sought at an early stage and if the decision is to bring in forensic cyber expertise, this contracting is best done via counsel as this may enable you to assert legal privilege in the experts’ findings.

When communicating, it is always best to use encrypted applications. It may sound counterintuitive but free apps such as Signal, Threema or Whatsapp are ideal. They offer simplicity, speed, usability and, crucially, end-to-end encryption.

What is very unhelpful is for executives to use systems such as Gmail – especially without multi factor authentication.

This is unfortunate because cyber criminals listen in to these conversations, compounding the problem for the victim company. And in fact, although multi factor authentication may sound trivial, it is certainly a frontline defence against attack.

Above all, never waste a good crisis. We always encourage clients to assess the incident and use learnings to improve systems and processes.

Insurance issues

Insurance is not a panacea. But it is a valuable component in a holistic risk management programme.

In essence there are two types of coverage available to companies and Funds alike: first and third party.

The former will help companies with incident management, from IT breach response services to public relations support; ransom negotiators and payments; business interruption; and possibly any fines or penalties you may incur.

But cyber-attacks often resonate along a value chain. And the latter type of coverage is for third party losses. For example, if a major IT supplier to your company is attacked and you experience business interruptions then you may be able claim for it.

Such issues work both ways. A victim company may face compensation claims for direct financial losses suffered by clients or customers. Or for damages for breach of contract. Or claims by data subjects whose personal data is compromised by the cyber-attack. The list goes on. Large numbers of tiny claims, or class action suits, can have a significant and material effect.

Working with your insurer, legal adviser and forensic expertise are just three aspects of reacting to cybercrime. Further conversations are necessary or advised.

If this is a personal data breach, you may be required to file a notification with the relevant data protection authority and the affected individuals may also be required to be notified.

Moreover, it is usually best practice to involve both law enforcement entities, financial markets supervisory authorities and, where appropriate,
Regulators.

The best form of defence is always prevention. Criminals are looking for vulnerabilities – patches that have been delayed for plausible reasons or insufficiently secure email access points. They are less likely to go for well-prepared companies. But whatever your situation, there are plenty of options to help you recover from an attack.

Managing data and cybercrime are complex and, at times, uncomfortable issues. At CMS our expertise includes a range of free tools to help any business in the UK and EU consider their preparations and response: a data law navigator, GDPR enforcement tracker and a breach assistant.