TOWERGATE INSURANCE BROKERS NEWSLETTER

ISSUE 16 WINTER CYBER RISKS EDITION 2021

END OF FINANCIAL YEAR? PRIME TIME FOR CYBER SCAMS

COMPARING A CYBER LOSS AND A FIRE LOSS

FUNDS TRANSFER FRAUD – A CASE STUDY

Cyber-crime still escalating - see our refreshed Cyber Hub CLICK HERE

CYBER RISKS SPECIAL EDITION

In a recent study, cyber risk features in the top three most important business risk, for the second year running. The Allianz Insurance Risk Barometer for 2021 shows businesses are facing a number of challenges such as larger and costlier data breaches, more ransomware incidents and the increasing prospect of litigation after an event. This compares with 2013 when cyber was considered the 15th biggest risk.

It is clear how quickly awareness of the cyber threat has grown, driven by companies' increasing reliance on their data and IT systems.

Cyber risks continue to evolve, with a significant increase in the number of ransomware incidents helping to drive up the frequency of losses to companies. Overall, cyber attacks are becoming more sophisticated and targeted as criminals seek higher rewards.

Towergate Insurance Brokers want to help you understand and navigate the changing risk landscape and have put together this special edition newsletter to help you combat the scourge of cyber crime.

We begin with an article published last year in the online publication Emerging Risks by Commercial Director, Mark Brannon.

THE EVOLVING NATURE OF CYBER RISKS AND CHANGING LANDSCAPE SINCE THE START OF THE PANDEMIC

With millions working from home in what was an almost instantaneous move to remote working in March, the cyber landscape changed overnight, while many were focused on other priorities says Mark Brannon, Commercial Director, Towergate.

This sudden, unforeseen and drastic change, combined with multiple distractions, presented a huge challenge for many organisations; and a prime opportunity for the cyber criminals.

In addition to the weakened 'offnet' infrastructure, home wi-fi and personal device vulnerability, employees' remote workings are more prone to human error. Many people will already be feeling vulnerable without colleagues around them to sense check an email, or may be multi-tasking care commitments and general distractions not faced in an office.

This shift in behaviours is pivotal, given around three quarters of cyber claims are caused by human error.

Like most common criminals, cyber criminals are opportunists and quickly exploited the situation, launching phishing attacks that prayed on employees' fears and vulnerabilities, including emails offering Covid-19 related tax relief, offering hand sanitisers and face masks, together with warnings about breaking new lockdown rules.

As Graeme Newman from CFC Underwriting has said for some time, "businesses in the cyber world are not targeted because they're valuable, they're targeted because they're vulnerable. And that is what a lot of smaller businesses miss." He has been proven right again.

Ransomware is a primary concern, which has become much more common and far more sophisticated. What used to be scattergun approached focussed on encrypting systems and preventing access is now more targeted and criminals are likely to also steal personal data held by the company. Threatening to publish it if the ransom isn't paid, this presents reputational risk, as well as a potential data protection fine and notification costs.

Another notable change is the ransom demands; not only has the amount substantially increased, but with the hackers often having accessed company accounts, they are also 'realistic' in the sense that the hackers know the company have the funds to pay and often make this known. As recently as three years ago the value of a typical extortion demand would average the low thousands but are now routinely high six-figure or million-pound extortion demands.

Another emerging trend last year has been cyber-attacks on managed service providers (MSPs), meaning there are huge vulnerabilities for businesses who outsource hosting or services to third parties now getting attacked where they become the victims caught in the crosshairs. Blackbaud was a perfect example of that in action in May, a socially good charitable hosting platform for charities, hospices and educational institutions globally, but the UK was disproportionately hit.

As always, prevention (or at least strong mitigation) is better than cure and is now crucial. Big data and the capability to scan customers, and scale within the market are becoming essential from an underwriting and performance perspective. It will not be sustainable for insurers to fund the losses being seen with a limited pool. Some markets that had dipped their toe are pulling out of cyber as the losses build against low price.

Risk management and claims infrastructure and response are key parts of the proposition; risk assessments, bulletins, best practice guidance and training are invaluable to ensure cyber security really forms part of a organisations culture. Education is key.

Many believe the pandemic is a blessing and a curse for the cyber risks faced with organisations going through short-term pain as they adapt to future working. It will lead to greater adoption of cyber security and is also changing perspective on insurance spend.

We will likely look back at this as a sea-change moment.

"RANSOMWARE IS A PRIMARY CONCERN, WHICH HAS BECOME MUCH MORE COMMON AND FAR MORE SOPHISTICATED"

END OF FINANCIAL YEAR?
PRIME TIME FOR CYBER SCAMS

The end of the financial year is a busy time for businesses as they race to achieve their numbers, with many finance teams preparing for the tax season. This creates a perfect environment for cyber security scams.

The most common are phishing related, where cyber criminals steal people's passwords and credentials. Seemingly legitimate emails trick recipients into divulging details, which then give the hackers access to the network posing as authorised users. Top-level executives are a prime target for these scams for a number of reasons.

Firstly, CEOs and other executives usually have clearance for all sections of the network. This makes their credentials more valuable.

Secondly, busy executives often don't notice that the email they've received is a scam because it looks legitimate. Because they're so busy and the email seems to be from a trustworthy source, they often click on the links without thinking twice.

Thirdly, the end of financial year is a time when businesses often receive emailed invoices and other communications, so a CEO, CFO, or even CIO is potentially more likely to take these at face value. Sometimes, attackers create fake invoices that look so real, businesses simply pay them. It then becomes incredibly difficult to recover those funds. Make sure you constantly vet your internal processes and keep communicating to help improve your cyber security defences.

The key to a more successful cyber security stance is a combination of technology, people and processes. And, while many businesses have now invested in strong cyber security technologies, a breakdown in processes and human error are often to blame for successful cyber attacks.

To avoid falling victim, business leaders need to instil a strong culture of security in the organisation. To be successful, this needs to come from the top down. If an executive doesn't take security seriously then neither will their staff.

To do this requires regular education for employees via training and informal reminders and tips. Businesses need to communicate frequently regarding current threats and standard safety procedures.

Successful training approaches go beyond focusing on compliance, which can be ineffective and not engaging for employees. Instead, companies should consider gamification to increase engagement and excitement around cyber security best practices.

You can go to our **Cyber Risk Assessment** to see if you are gambling with your cyber and data security and watch a **short video**.

It's also important to create an open culture when it comes to reporting potential breaches. Creating a punitive atmosphere only discourages people from coming forward in time to fix the vulnerability. Instead, organisations should praise staff for coming forward, then move quickly to address the breach.

Technology can help augment the people-based approach. For example, threat intelligence tools can automatically identify phishing sites and prevent employees from visiting them. This can help prevent leakage of password-based credentials to unknown sites, even if they aren't officially categorised as phishing sites. Businesses should also use policy-based multifactor authentication enforced at the network level.

Importantly, everyone in the organisation, but especially management, must be aware that the end of the financial year is a peak time for cyber security scams. They need to remain extra vigilant during this time and refrain from clicking on links in emails, regardless of how legitimate they may look.

While your company should be ahead of the curve with security technology, making sure your people are aware of scams and trained and your processes are solid, can make your financial year end on calmer waters.

Are you gambling with your cyber and data security? Click here to try our **Cyber Risk Assessment**

COMPARING A CYBER LOSS AND A FIRE LOSS

No one wants to have to claim on their insurance. All losses have a detrimental affect on individuals and businesses alike. They can affect business continuity, lead to loss of reputation and, at worst, imperil the very existence of companies.

With the rise in cyber crime, there has been a rise in insurance claims. Businesses may not be at ease with this sort of claim as they may not have experienced these before. Cyber crime is insidious, unseen and potentially multi layered and complex. With other physical losses such as fire, it is likely that you will have a good idea as to what to do in the event of a claim.

Cyber can feel more complex due to it being a newer risk and its intangible nature. We have put together the instructive table below which outlines the how a cyber loss can be more similar to a more traditional fire loss than you might first think.

FIRE LOSS	
Electrical fault causes massive fire at head office premises	
IMMEDIATE REACTION	**IMMEDIATE CONSEQUENCE**
Fire needs to be extinguished	Building cannot be accessed
SECONDARY REACTIONS	**SECONDARY CONSEQUENCES**
Alternative office space is required	Alternative accommodation requires paying extra rent
Cause of fire needs investigating	Loss adjusters costs
	Investigations take up management time
New equipment needs to be purchased	Funds required for new equipment
Offices need to be rebuilt	Funds needed to rebuild/repair damage depending on the severity of the fire
Office fit out	Funds required for replacing lost contents
Lost time in having no offices	Overtime required to catch up with the down time to minimise impact on business
Lost Sales	Having no office, can result in a direct loss of custom, new orders cannot be taken, existing orders delayed direct impact to cash flow
	Business moves to competition
Crisis containment/PR	In the event of a fire loss, a company would want to reassure its customers that it's still able to trade and fulfill requirements to help minimise the damage to a company's reputation and any loss of trading. This could extend to any environmental impact and responses may include a formal communication strategy to running a 24/7 crisis press office, depending on the severity.
Fines and Penalties	H&S investigations, possibility of fines/prosecution

CYBER LOSS	
Employee clicks on malicious link and systems are encrypted	
IMMEDIATE REACTION	**IMMEDIATE CONSEQUENCE**
Virus needs to be removed from the system	IT systems cannot be accessed
Pay the ransom	Immediate financial loss
Decline to pay ransom	Data is lost, corrupted or irretrievable
SECONDARY REACTION	**SECONDARY CONSEQUENCE**
Alternative means of communication and working required in the short term	Labour intensive, creates large amounts of offline information
Cause of computer failure needs investigating to prevent reoccurrence	Specialist IT forensic teams highly expensive
	Investigations take time, systems still not accessible
New "clean" equipment required that is virus free	Some equipment might be irrevocably damaged in the attack and needs replacing
Systems need rebuilding, data needs to be reconstructed	Takes time. Data which cannot be restored from backups needs to be manually restored. Labour intensive extra staff required
System needs testing to see if they work before roll out.	Creates time delays and prevents use of systems, compounding extras costs once systems are restored
Lost time in having no systems	Overtime to catch up, all the information created offline now needs to be entered back on to the system
Lost Sales	No IT systems means new orders cannot be processed, existing orders are lost, invoices cannot be generated and sent out, direct impact on cash flow
	Business moves to competition.
	Cancelled contracts
Crisis containment/PR	In the event of a data breach, prompt, confident notification and communication is critical to help minimise the damage to a company's reputation. Responses may include a formal communication strategy to running a 24/7 crisis press office, depending on the severity.
Fines and Penalties	GDPR/ICO investigations and penalties PCI Investigations and fines

To see some of the cyber threats you face, click here to watch our cyber video.

FUNDS TRANSFER FRAUD - A CASE STUDY

Funds transfer fraud – whereby fraudsters dupe innocent businesses and individuals into transferring what they believe are legitimate payments to fraudulent bank accounts – is becoming an increasingly common problem for most modern organisations.

However, it's not always a business that can suffer a loss in this way, but it's customers too. Customer payment fraud describes a situation in which a business is impersonated by a fraudster, who then dupes some of the business's customers into making payments to a fraudulent account.

One business affected by such a loss was a private, tuition-paying school responsible for educating 11-18 year olds. The school in question has boarding facilities in place and attracts students from many different countries around the world.

Lack of multi-factor authentication lets fraudster in

The scam began when the school's bursar, the individual responsible for managing the financial affairs of the school, fell for a credential phishing email. Credential phishing emails are used by malicious actors to try and trick individuals into voluntarily handing over their login details, typically by directing them to a link that takes them through to a fake login page.

In this case, the bursar received an email from what appeared to be Microsoft, stating that if he wanted to continue to use the email account without interruption, he would have to validate his account details online. Not wanting to face any disruption to his work, the bursar clicked on the link provided, which took him through to an authentic-looking landing page where he inputted his email login details and gave no further thought to the matter.

Despite appearances, however, the landing page was actually fake, and the bursar had unwittingly volunteered his email login details to a fraudster. What's more, his email account didn't have multi-factor authentication in place, so the fraudster was then able to access the account remotely and gather valuable information. In particular, the fraudster was able to locate a spreadsheet stored in one of the bursar's email folders containing a list of email addresses for the parents of current students, which was typically used for distributing general messages and updates from the school.

MFA is an authentication process that is used to ensure that a person is who they say they are by requiring a minimum of two pieces of unique data that corroborates their identity. Most cases of business email compromise could be prevented by implementing it.

Scam initiated with offer of discount

Having spotted an opportunity, the fraudster moved on to the next stage of their scam. Their first step was to set up an email address that looked substantially similar to the bursar's, but with the addition of an extra letter to the address line. So instead of saying @abcschool.com, it became @abcscchool.com. The next step was to carefully select which parents to target. Rather than adopting a scatter gun approach and emailing every parent on the list, the fraudster specifically selected parents based overseas. This was presumably done not only on the basis that such parents are more likely to be paying both tuition and boarding costs (thereby making them more lucrative targets), but also in the belief that overseas parents might be more likely to fall for the scam and less likely to raise the alarm to the school.

With the targets selected, the fraudster sent out an email relating to the payment of school fees. The email began by outlining what the annual fees for tuition and boarding amounted to, but then stated that parents would be eligible for a discount of up to 25% if they paid for the spring and summer terms in one lump sum as opposed to paying separately at the start of each term. To add a sense of urgency to making a payment, the email then went on to say that there was a deadline for payment in place, after which the discount would expire. Social engineering attacks rely on manipulating and exploiting typical human behaviours, and in this case the fraudster was clearly aware that the scam would have a better chance of success if the parents were provided with a financial incentive to make the payment within a set time frame.

In addition, the email was well thought through and included a number of features to make it appear more authentic. For example, not only did the fraudster use proper spelling and grammar and include the bursar's genuine email signature, he also went on to state that if the student was unable to complete the academic year for whatever reason, then the fees would be reimbursed on a pro-rata basis.

School's security breach puts parents out of pocket

Unfortunately, this offer proved to be too tempting for some and six parents fell for the scam, transferring the tuition and boarding fees over to the fraudulent account details provided on the email. With tuition and boarding fees at the school costing some £10,050 per term, the amount paid out by each parent at a 25% discount amounted to some £15,075.

It was only after a few days, when one of the parents that had received the email forwarded it to one of the school's administrators to check the validity of the discount offer that the school became aware of the scam. The school immediately notified all parents about the scam and urged them to be aware of any suspicious emails that appeared to have come from the school.

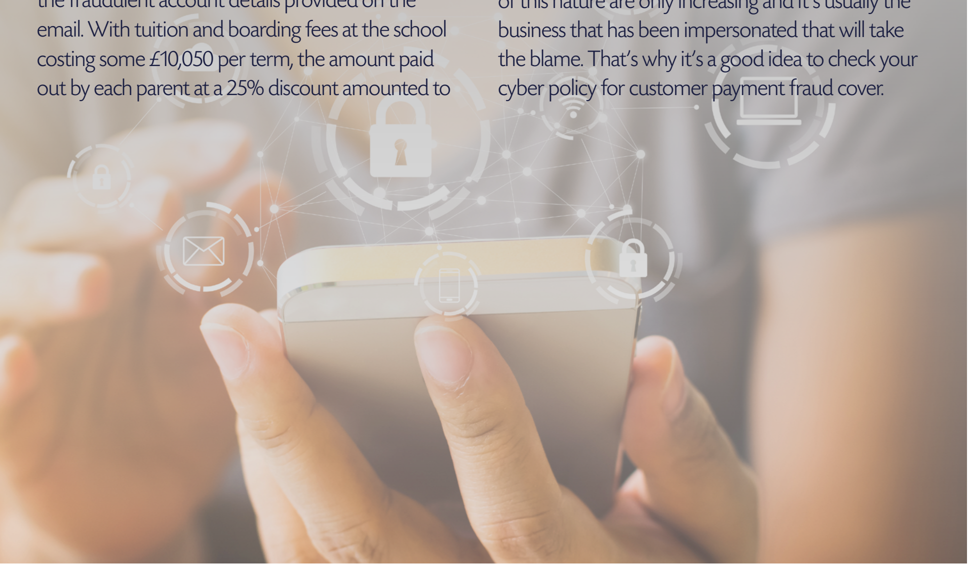
Of the six parents affected, just two were able to get their money back

The parents that fell for the scam reported the incident to their respective banks to see if the transaction could be either frozen or reversed, with mixed results. Of the six parents affected, just two were able to get their money back, with the rest left out of pocket to the tune of £60,300 collectively.

As it was a compromise of one of the school's email accounts that had allowed the fraudster to gain access to the parents' email addresses, the school felt morally obliged to reimburse those parents affected by the fraud. Fortunately, the school was then able to recoup most of this loss under the cyber crime section of its policy with CFC, which provides cover for customer payment fraud up to a maximum of £50,000.

A lesson learned

This case study highlights the need for customer payment fraud cover in cyber policies. Many cyber policies with crime sections will only provide cover for losses that directly affect a policyholder. But in this instance, it wasn't the school that suffered a direct loss but its customers. However, because it was a compromise of the school's computer systems that allowed the attack to be carried out, the school felt duty bound to reimburse the parents affected. With more and more financial transactions being carried out electronically and with more and more cyber criminals looking to intercept them, the chances of a business's customers falling for scams of this nature are only increasing and it's usually the business that has been impersonated that will take the blame. That's why it's a good idea to check your cyber policy for customer payment fraud cover.



Case study supplied by CFC Underwriting

CYBER INSURANCE RATES INCREASE PREDICTED FOR 2021

Cyber insurance capacity is expected to reduce with some insurers exiting the cyber market, resulting in higher rates, as insurers encounter both a higher frequency and severity of claims.

As the frequency and sophistication of cyber attacks has increased, there is mounting pressure on insurers to increase rates and underwriters to be more selective with risks.

An increase in the severity and the rising number of ransomware attacks is seen as one of the biggest challenges for the cyber insurance market. There is a consensus in participants that rates will need to rise with a correction in certain segments which have been underpriced in previous years. This may also be accompanied by adjustments to underwriting terms.

In the past, buyers were able to renew their insurance with little information required, however, they will have to work harder now. They should take this opportunity to improve and articulate their management of their risk positions to achieve the best terms possible.

The growth of ransomware and other threats have not made it easy on carriers. They will need to keep up and improve their technical expertise to enable clients to protect themselves from cyber crime.

"This year we'll see a shake-up in the market in terms of who wants to continue to write cyber as a class of business and to do so in a meaningful way, providing a service that clients will want to buy," Lindsey Nelson, Cyber Development Leader at CFC Underwriting said. "The best positioned cyber insurance markets who will be long-term partners will be those who continue to invest in their in-house cyber claims infrastructure, where there is a mutual interest in ensuring claims are handled effectively without incurring unnecessary costs. Luckily, cyber insurance is one of the few lines of insurance where we can work to prevent claims before they happen, providing clients with proactive threat alert scanning from the first day of binding.

Ransomware will continue to be one of the biggest threats to UK businesses in 2021, and as the cyber market continues to look for rate and react to the severity of these losses, the cyber providers who have the size, scale and expertise in the market are going to be best placed to be a consistent and stable solution for clients.", Nelson added.

At Towergate, we know capacity is available and will work hard to secure the best cover and terms. Clients need to make sure they have expert insight into the market and that comes with having the right broker so they can make sure the market can work to their advantage.

For more information, please contact your usual Towergate Advisor or email:**TIB@towergate.co.uk**

towergate
Insurance Brokers

Towergate Insurance Brokers is a trading name of Towergate Underwriting Group Limited. Registered in England with company number 4043759.
VAT Registration Number: 447284724. Registered Address: 2 Minster Court, Mincing Lane, London EC3R 7PD. Authorised and regulated by the Financial Conduct Authority.

The information contained in this bulletin is based on sources that we believe are reliable and should be understood as general risk management and insurance information only. It is not intended to be taken as advice with respect to any specific or individual situation and cannot be relied upon as such.