Commercial Risk
Insurance & Risk Management News

JLT

RANSOMWARE
TO PAY OR NOT TO PAY


TARGET
TARGET
TARGET
TARGET
TARGET

LOSS PREVENTION & RISK MANAGEMENT

It is now widely recognised by most risk management and IT security professionals that it is not a question of if, but when a cyber-attack will occur.

Companies rightly invest in building walls around their systems because preventing access in the first place is an obvious building block for an effective defence strategy against ransomware. Most companies still use very weak and out-dated commercial cyber security software, forgetting that the threat is often internal. They often focus their energy on shoring up their defences against an increasingly sophisticated, and at times, state-backed enemy invading force instead. The key is to make sure that your first line of defence against an attack is backed up by a structured and enterprise-wide approach to managing and mitigating the risk, so that the reputational and financial impact is minimised as much as possible.

The ransomware experts gathered for this discussion agreed that most organisations, including at the top board level, are thankfully becoming more aware of the scale and realities of this risk quickly. Awareness of this issue has been boosted by the introduction of rules and regulations, such as the EU's General Data Protection Regulation (GDPR), which came into force across Europe last year. It was then further aided by the reporting and governance requirements introduced specifically for cyber by the Financial Conduct Authority (FCA), which were implemented in the UK financial sector.

The FCA has made it crystal clear that it wants to see an organised and structured approach to this risk, not a tick box approach. This demands leadership from the top. The key assets and vulnerabilities need to be properly identified, measured and prioritised with budget allocated accordingly on an ongoing basis. Our roundtable experts recommended allocating an element of the cyber risk budget to ongoing staff training and involving human resources (HR) in the risk strategy for it to prove most effective.

Our risk management and IT security professionals agreed that, as with all attempts to prevent, manage and mitigate business-critical risks, this is not just about structures, systems and reporting. The most important point of focus has to be the culture, education and awareness of all staff from top to bottom of the company, across all functions and departments. As cyber is very much a human risk. Humans are the vulnerable parties and weak links in the cyber security chain. A company may spend a fortune building the most fool proof firewall possible, but, if staff are not trained and encouraged to spot the dubious email arriving in the first place and made aware of the potential impact of clicking on that link, it will have all gone to waste.

When cyber risk first emerged, the IT department generally took ownership of the risk. Attempts to 'help' offered by other functions, such as risk, legal and audit, were often rebuffed because they were seen as criticisms of the IT team's ability to do their job. Thankfully now it appears that, along with the rising role of the Chief Information Security Officer (CISO), there is a fast-growing understanding that everybody 'owns' cyber risk. All staff must play their role in preventing attacks from happening in the first place and then help to mitigate them when they inevitably occur. Our panellists were clear that senior business leaders should give sufficient attention to the potential threat this weak human link could pose to the company, rather than delegating the responsibility for this risk solely to the IT department.

KEY TAKEAWAY POINTS

The following key takeaway points, from the JLT/Commercial Risk Europe roundtable, sum up the key risk issues and responses required by the FCA on loss prevention and risk management:

RECOGNISE THAT HUMANS ARE THE CORE VULNERABILITY

John Harrison, Head of Information and Cyber Security at Charles Stanley: *"There is a person in the chair and, no matter how many protective mechanisms are in place, people are fallible and may, in a moment of weakness, click on the phishing link. These links have become so much more sophisticated, targeted and relevant, appealing to basic human traits such as greed and fear. Apathy is also a factor. People hear so much about cyber- crime and ransomware attacks. They are asked to strengthen their passwords and not to click on links etc., but they may still be complacent thinking their company has systems in place to protect them."*

Ffion Flockhart, Norton Rose Fulbright's Global Co-Head of Data Protection, Privacy and Cybersecurity: *"It's right that greed and fear are the basic human emotions targeted. The most successful attacks include those where HR is impersonated, especially when it occurs during the pay round process. People are told to click a link and give their username and password to find out what their annual bonus will be. Another one that works is a message from Inland Revenue telling an individual about a fine or tax rebate."*

COMPETING FOR VALUABLE TIME CAN BE CHALLENGING

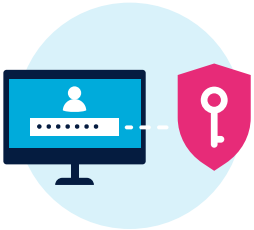
John Harrison, Head of Information and Cyber Security at Charles Stanley: *"It can still be difficult for security teams to secure top level engagement when it comes to cyber risk. We have an interested and actively involved Senior Management team at Charles Stanley, but if a firm was to have a CEO who wasn't genuinely engaged, it would be almost impossible to secure the necessary buy-in and commitment from the rest of the organisation. Genuine top level management interest is vital.*
The problem is that there are so many demands on the Board's time: general risk, cyber, compliance, data protection, governance and, of course, running the business on a day-to-day basis. There can be an element of fatigue that needs to be taken into consideration, and the approach to secure engagement should be adapted accordingly."

REGULATIONS HAVE HELPED RAISE AWARENESS AND FORCE POSITIVE ACTION

Sarah Stephens, Head of Cyber/Technology E&O at JLT Specialty: *"The implementation of the General Data Protection Regulation (GDPR) in May 2018 significantly increased the financial consequences of ignoring data privacy and protection. Companies are now taking a more proactive approach to their risk management strategy and further educating themselves on the various cyber threats facing them. This increased awareness has already resulted in more investment in cyber security, which should act as a deterrent for hackers who seek easy targets."*

ACCEPT THAT THEY WILL BREAK THROUGH THE PERIMETER AND PREPARE ACCORDINGLY

Winston Krone, Global Managing Director at Kivu Consulting: *"A lot of the time companies have not lost everything, only a certain part of their data. Then the question is whether it is worth retrieving. An important factor to consider is whether their data is backed up or not. If it is not properly backed up, or if the attackers have been allowed to access and delete those backups, then that is what you will be paying for."*



EDUCATION IS CRITICAL – CARRY OUT TESTS

Munesh Vadher, Director Cyber Risk at Barclays: *"Don't forget that ransomware is targeting customers as well as large companies, so education and awareness on an individual basis is key. As part of our Digital Eagles programme to help small businesses and communities grow and develop, we run awareness campaigns through media channels and workshops to help educate people to become more aware about being safe online, the threats out there and what they need to do to defend themselves."*

BOARD BUY-IN IS NEEDED, BUT THIS CAN BE A CHALLENGE

Ffion Flockhart, Global Co-Head of Data Protection, Privacy and Cybersecurity at Norton Rose Fulbright: *"This can be quite a challenge for many leaders. Remember Marissa Mayer, former CEO of Yahoo who was in charge when the group had to disclose the biggest cyber breach in history, ultimately had to step down. The Yahoo breach affected up to 3 billion accounts worldwide, led to class actions and devalued the company by USD 350m. You need commitment from the top and for cyber risk to be managed at executive level, not just a small group within IT. A budget must be set aside specifically for information security."*

THE BIG QUESTION

TO PAY OR NOT TO PAY REMAINS AN OPEN QUESTION

It is legal in most countries of the world to pay ransom demands for valuable data to be returned from criminals. The core question is actually a commercial one:

"Is the price of the 'deal' worth it? Is it really worth paying an outrageous amount for their return on your offer?"

There are potential complications that need to be carefully evaluated with the support of experts, such as whether such a payment could actually contravene international regulations on money laundering and the funding of terrorism. It is also important to follow the right steps and procedures to show that you have made every effort to ensure that you are not breaking any rules and regulations that could lead to future fines, reputational damage and, of course, the invalidation of your insurance cover. These were the core conclusions of the panel of experts gathered by JLT Specialty and hosted by Commercial Risk Europe to discuss this increasingly important problem.

"Assuming your regulatory due diligence pans out, this is a business decision," said Winston Krone, Global Managing Director at Kivu Consulting, the firm that advises victims of ransomware on how to react and helps them to negotiate the best 'deal'. "We work with clients to reach the right decision in very stressful circumstances. We identify whether the data is needed, how long it will take to decrypt, the extent to which it will be permanently corrupted, and the actual likelihood of getting it back at all. There are a lot of factors to be taken into consideration. Whether to pay or not can be a red herring. The big question is do you need the data and is it worth paying to get it back," continued Mr Krone.

Ffion Flockhart, Global Co-Head of Data Protection, Privacy and Cybersecurity at international law firm Norton Rose Fulbright, said that there is no specific law, at least in the UK, that prohibits the payment of ransom demands, but advised victims to consider wider areas such as sanctions and terror funding. "Whether the ransom funds terrorism or breaks sanctions is a question to be taken seriously. Knowingly paying a terror group is illegal under UK Terrorism legislation and there can be severe penalties for making payments to those on a sanctions list. This is clearly an important factor and you are advised to get forensics on board to help ascertain the likely identity of the attacker," she explained.

Anti-Money Laundering (AML) rules are also of concern, particularly for the financial sector, added Ms Flockhart. "Another element that is tying the financial sector up in knots is the AML rules. However, ransoms only become the proceeds of crime once they are received by cyber criminals, so the actual payment of a ransom, at least in the UK, would not of itself be a money laundering offence," she explained.

According to the experts on this panel, leading law enforcement agencies, such as the FBI in the US and the UK authorities, do not openly encourage companies to pay ransoms. However, they will increasingly turn a blind eye, so long as the ransom is not clearly funding terrorism. "You will never get a rubber stamp from the FBI or other authorities. You also need to be careful – it is illegal to pay ransoms in some countries and, in others, you may find that notifying the authorities leads to your servers being requisitioned. You need to do your homework and take good advice," responded Ms Flockhart.

Another panellist pointed out that in some countries, notably Italy and Mexico, the law can be confusing because it is linked closely to kidnap laws, so again care must be taken when deciding whether to pay up or not. Winston Krone of Kivu said that any responsible company will make sure that they are complying with all the relevant rules when in these situations, but stressed that, at its root, this is a business decision that needs to be weighed up in the normal way.

“We are generally only brought in when it is bad. A lot of the time companies have not lost everything, only a certain part of their data. Then the question is whether it is worth retrieving. An important factor to consider is whether their data is backed up or not. If it is not properly backed up, or if the attackers have been allowed to access and delete those backups, then that is what you will be paying for,” he said.

Mr Krone and Ms Flockhart agreed that another very important consideration when trying to work out whether to pay up or not is the reliability of the criminals. “The dark web effectively has its own version of Trip Adviser for ransomware criminals, which shows their reliability for returning the data and their technical ability to hand it back,” explained Ms Flockhart. So, if the criminals themselves are graded on the dark web, are companies also graded for their willingness to pay? Would their grade potentially make them vulnerable to future copy-cat attacks? Not so, agreed the experts.

“This is a myth,” said Mr Krone. “The attackers do it because they’ve found a way of getting into that particular system. Usually companies that have been hit already are more difficult to hit again because they tend to be wiser, as they have already been through a very expensive and stressful training exercise,” he continued. “Where a ransomware victim gets hit again, it’s almost always because they failed to patch the original vulnerability or else didn’t properly clean their infected network.”

Another really important consideration, when trying to work out whether it’s worth paying, is to actually know what you are paying for, added Ms Flockhart. “Too often people do not actually know what is in the dataset that they no longer have access to. Clearly knowing what is actually there is vital!” she said.

DEDICATED POLICIES, CLEAR EVIDENCE AND A PARTNERSHIP APPROACH ALL HELP TO ENSURE THAT CLAIMS ARE PAID IN RANSOMWARE CASES

If risk managers want to make sure that their cyber claims are paid without fuss and in good time, they need to purchase dedicated cyber cover, rather than relying on existing standard policies for their silent cover. Relying on a kidnap and ransom policy to help deal with a ransomware attack may lead to coverage disputes. It can also mean that the insurer provides the company with a kidnap negotiator, rather than a cyber expert, to help them deal with the problem.

When the ransomware claim inevitably hits, it is also absolutely critical to gather and save the relevant details and notify your insurer and broker as soon as possible. You must also make sure that the IT department does not take it upon itself to try and fix the problem before telling anyone else about it. If the evidence of the attack is inadvertently destroyed in the immediate aftermath of the incident, seeking full recovery will be made all the more difficult.

These were some of the key conclusions reached by the group.

Sarah Stephens, Head of Cyber / Technology E&O at JLT Specialty, said that negative claims experience remains relatively limited in this young, but fast-growing market. Claims have generally ended in positive outcomes for customers. Any problems that do emerge tend to occur when the company relies on

standard non-cyber policies coverage and hopes that it will cover cyber risk, she explained. “We have not seen that many declined claims, and what we have observed overall is really good claims behaviour in the market, which is encouraging. CFC Underwriting, the specialty underwriter in the market, has published good data in this respect. The data shows that claims denial is 1-2% in cyber, compared with 15-20% across their overall book. When you look at the details, you generally find that publicised ‘cyber coverage denials’ are related to other policies like crime or professional indemnity, not dedicated cyber policies,” explained Ms Stephens.

The obvious advice for any company that seeks to secure robust and reliable cover for ransomware and other cyber risks is to take out a dedicated cyber policy. Then carefully construct the cover in partnership with the broker to make sure it reacts as intended when the claim inevitably hits. “Problems with claims tend to arise when there is a fundamental disconnect between what the company wants and needs and what the policy provides. Historically companies would perhaps use a kidnap & ransom policy to try and cover a ransomware attack. However, these policies were designed to cover executives, not cyber attacks, and so this can cause disputes. Moreover, you will want help from an expert ransomware negotiator, rather than an expert kidnap negotiator! It is best to opt for a dedicated cyber policy to address the bulk of cyber risk,” added Ms Stephens.

All business insurance claims run more smoothly if the evidence regarding cause of loss is gathered quickly and efficiently as soon as the event occurs. As with any serious crime incident, any efforts to ‘clean up’ too quickly, and often clumsily, will inevitably lead to future problems. The need to carefully document and store the evidence as rapidly as possible is perhaps more important with ransomware incidents than any physical loss, as the incident moves so quickly.

Claire Combes, Board Member at UK risk management association Airmic and Director of Risk & Assurance at intu, the owner and manager of some of the UK’s most popular shopping destinations,

said that clear communication on this important matter is needed to ensure 'evidence' is not lost at the early stage. "A common problem faced by some companies is that IT teams want to react immediately to the problem and won't necessarily think about notifying insurers and using the support they can provide under the insurance policy. Protocols have to be followed or claims can be invalidated."

"To help with this, at intu we hold cross functional meetings with the insurers and relevant departments such as ICT to fully understand the coverage provided and how this would benefit the business when activated" she explained.

Ffion Flockhart, Global Co-Head of Cyber Risk, Norton Rose Fulbright, pointed out that it is in everyone's interest to work together as closely and transparently as possible with such claims. Particularly if the insurer also provides value added services, such as crisis management and access to skilled negotiators. The desires of both the customer and insurer need to be clearly aligned to contain the loss, stressed Ms Flockhart.

AMATEUR RANSOMWARE ATTACKS ARE ON THE RISE, BUT DON'T EXPECT THE 'MARKET' TO KILL ITSELF

The experts gathered by JLT Specialty to discuss the increasingly important area of ransomware agreed that the easy access to the software needed to carry out the attacks before demanding the 'ransom' has attracted more amateurs into the market. These rookie hackers may simply be incapable of delivering on their promise to return the stolen goods or access to the 'kidnapped' data.

Prices for the ransomware weaponry, available on the dark web, are also falling, as competition among providers rises. This means that companies held to ransom really need to seek support from experts in the area, who can help them work out whether the ransom is actually worth paying and whether the criminal will actually be capable of delivering the goods.

Fellow panellists asked what percentage of companies actually have their data successfully returned after paying the ransom. Winston Krone, Global Managing Director at Kivu Consulting, a firm that specialises in negotiating with ransomware criminals, said that it really depends on the victim's ability to identify how 'reliable' the criminal is.

"The return rate is actually about 99.9%, but this is kind of self-fulfilling because we will not pay a ransom unless we are as sure as we can be that it will be successful. If we do not think that the client will achieve a positive return and the data will be returned, then we will warn them not to pay. This year we have seen a rise in the number of complete amateurs getting into it. Technically they do not know how to do it. We have seen cases in recent times where criminals have had their license cut off by the provider half way through the negotiation because they have been asking too many questions!" explained Mr Krone. The negotiating expert recalled an incident where his company was forced to go directly to the provider on the dark web to try and find a result that the criminal could not achieve.

Mr Krone added that part of the process is to work out whether or not the data is actually worth the risk of the exercise; "Probably in 20% to 25% of cases, the ransom is not worth paying because of the likelihood of not getting the data back."

ABOUT JLT SPECIALTY

JLT Specialty Limited provides insurance broking, risk management and claims consulting services to large and international companies. Our success comes from focusing on sectors where we know we can make the greatest difference – using insight, intelligence and imagination to provide expert advice and robust – often unique – solutions. We build partner teams to work side-by-side with you, our network and the market to deliver responses which are carefully considered from all angles.

As a Specialty Broker, we already know the available insurance products inside out, but we make it our mission to also understand the industry sectors and businesses we work with. Cyber risk is universal; we want to ensure that we fully understand the impact Cyber incidents can have on you. Considering the nature and level of misinformation surrounding Cyber and Technology Errors & Omissions, many clients can't comprehend the intricacies of the product. We're here to share our knowledge with you and your company, including helping you to present the information to your C-suite.

Cyber' can seem daunting and complicated concept, but it doesn't need to be. We're here to help you understand the specific risks your company faces and find you the insurance solution that caters to your individual needs. We can clarify any misinformation you have received and demystify the boundaries of cyber risk, helping you to decide which cyber loss scenarios are most relevant to your company and what your risk picture looks like. We can highlight exactly what is covered under a cyber insurance policy to ensure that you feel confident when choosing the right policy for you. Our team can also help to improve your company's cyber security awareness, so that your employees and C-suite remain vigilant against any potential threats.

CONTACTS

SARAH STEPHENS

Head of Cyber / Technology E&O

+44 (0)207 558 3548

sarah_stephens@jltgroup.com

JLT Specialty Limited

The St Botolph Building
138 Houndsditch
London EC3A 7AW

Tel: +44 (0)20 7528 4444

www.jlt.com