airmic

GUIDE 2024

Cyber Claims

IN ASSOCIATION WITH:

bakertilly S-RM Paragon

About Baker Tilly
Baker Tilly is a leading advisory, tax and assurance firm, providing clients with a genuine global advantage. Our integrated team of experienced and credentialed professionals work on multifaceted financial matters, providing accurate and reliable financial analysis to organizations seeking clarity in complex situations. Attorneys and their clients turn to us for the financial understanding and expertise necessary to develop effective strategies that resonate, educate and persuade from the courtroom to the boardroom. From economic and financial analyses, to valuation, to litigation support and expert witness testimony, we deliver at every phase.

www.bakertilly.com

bakertilly

About S-RM
S-RM is a leading global cyber security and corporate intelligence consultancy. Founded in 2005, we have 400+ practitioners serving clients across all regions and major sectors. We design, implement and test cyber security programmes that align with our clients' mission and strategic objectives; support them through cyber incidents by helping them to recover swiftly and emerge more resilient; and provide insights on the cyber security risks to investment targets and portfolio companies. Headquartered in London, we have offices in Cape Town, Utrecht, Hong Kong, Singapore, New York, Washington DC, Manchester, and Kuala Lumpur.

www.s-rminform.com

S-RM

About Paragon
At Paragon we know that there is no 'one size fits all' insurance approach. We understand the distinct needs of architects, directors, lawyers, healthcare professional and more. Our experience paired with our exceptional knowledge within the industry allows us to foresee and manage the unique risks posed by cybercrime, mergers and more. Our approach to insurance strategies exceeds our clients expectations. From startups to global enterprises, we provide tailored solutions with a personal approach.

Paragon

About Airmic
Airmic is the leading UK and Ireland association for everyone who has a responsibility for risk management and insurance in their organisation, Airmic has over 450 corporate members and more than 2,000 individual members. Individual members are from all sectors and include company secretaries, finance directors, and internal auditors, as well as risk and insurance professionals. Airmic supports members through learning and research; a diverse programme of events; developing and encouraging good practice; and lobbying on subjects that directly affect our members and their professions. Above all, we provide a platform for professionals to stay in touch, to communicate with each other, and to share ideas and information.

www.airmic.com

airmic

Airmic guides are provided to give an insight and some understanding into different areas of risk. They are not intended to address any particular requirements or issues. Airmic guides are not intended to replace the need for advice nor are they training guides. Airmic does not accept any liability for the content of the guides which are prepared based on the views of the author (who may not be an Airmic employee).

CONTENTS

01 Foreword

With each passing year, more and more organisations are experiencing first-hand how costly ransomware attacks can be in terms of time, energy and money. Behind the scenes, large cyber insurance claims are often an underpublicised source of stress for these organisations, many of whom may wish in retrospect that they had taken proactive steps that would have made the cyber claims process more efficient and more cost-effective.

The reality is that ransomware attacks are continuing to occur at an alarming rate. The cyber problem has become a global crisis – no nation is immune at this point. Regardless of what country you live, work or operate a business in, you need to be aware of common mistakes that unite organisations that have fallen victim to ransomware attacks, and the steps that you and your business can take to pave the way for a smooth cyber claims process.

The mistakes that organisations make during a cyber claim range from minor issues causing minimal damage to significant errors that result in catastrophic financial losses, not to mention the cost to those organisations in terms of time, energy and reputation.

S-RM recently conducted a comprehensive study in which the global intelligence and cyber security consultancy firm analysed nearly 450 cyber incidents over a 12-month period and then rated 21 factors by frequency and average impact on costs. This white paper discusses several of these themes.

Drawing on the combined insights of S-RM, Baker Tilly US and Paragon Brokers across thousands of incidents, this white paper highlights the best practices and common pitfalls faced by organisations preparing for cyber incidents, and their resulting claims processes.

01 FORWORD

02 Preparing for a potential attack

The central theme of this white paper is preparation. When your organisation prepares thoroughly for the possibility of a cyber incident, you are infinitely less likely to suffer significant financial losses and waste your time (and others' time too), and generally less likely to endure a chaotic claims process.

It is not hyperbole to say that almost every issue that arises in the cyber claims process typically results from poor planning. Not only does planning create a solid foundation within an organisation, but it also sets the tone for how it will respond to adversity.

Incident response planning

An organisation's incident response plan is essentially a continuous cycle that includes the following five steps:

- Planning for a crisis
- Crisis management
- Process adjustment
- Gathering feedback
- Planning for a future crisis (using lessons learned).

Simplicity is key to effective incident response, as is being clear in each stakeholder's role in the process. With this in mind, organisational leaders should sit down with their IT teams, lawyers, insurance brokers and other key professionals to map out incident response plans as early as possible. This includes reviewing all relevant questions, such as:

- What are your options, in the event of a cyberattack?
- At what point do you need to notify your insurance broker/insurer?
- What are your objectives as you look to recover?
- What will you do with your current applications?
- Are you going to reinstate on premises, or in the cloud?
- Will you reinstate as is, or are hardware and software upgrades required?

With these questions in mind, not only is it important to prepare your organisation for a possible cyber incident, but it is also pivotal to prepare your vendors, your insurance company, your accounting firm and other key business partners that will be involved should you fall victim to a ransomware attack.

Using this mindset, you need to consider how a cyber claim would likely be handled, for example:

- Who is going to do what? What will be the roles and responsibilities of key stakeholders in your response – senior management, your insurance brokers, in-house and external lawyers, IT vendors and other professionals?
- Do you have a detailed understanding of your infrastructure, including a comprehensive network asset diagram?
- From a reinstatement perspective, do you know which applications are critical for revenue generation and which servers they are on? Does the reinstatement plan prioritise these servers and applications?
- Do you fully understand your insurance policy? Have you walked through potential scenarios (both internally and with your broker) ahead of time to identify where coverage issues may arise that may delay potential settlement if not clarified prior to an incident occurring?
- What vendors are you going to use? What vendors will your insurers require you to use? Will additional consultants be required?

As part of its research, S-RM highlighted the importance of effective coordination between all parties as one of the central factors that can reduce the overall cost of a claim. In S-RM's study, organisations experienced higher costs when multiple IT and digital forensics vendors were engaged to support the response without being effectively coordinated. The result was invariably duplicated efforts and costs, mixed messages about key investigation findings, friction within the claims process and, ultimately, slower and more costly recoveries.

In preparing for a potential cyberattack, organisations generally focus on IT, legal and PR (which is natural because, after all, it is a crisis). But while those areas require significant attention, not enough time is typically spent on how to pull everything together from an insurance standpoint, not to mention the elements of an insurance claim that involve outside vendors.

In reality, everything needs to be planned for in advance so that the most important information (what is happening and who is doing what at a given time) can reach the insurers, forensic accountants, lawyers and other key people as quickly and clearly as possible.

02 Preparing for a potential attack

Risk presentation

An often-misunderstood element of risk is that you need to be able to explain the true nature of risk in an understandable way in order to transfer that risk to someone else. So, you need to present your situation to insurers clearly and thoroughly. Standard insurance proposal forms – and the closed nature of a number of the questions contained therein – typically don't lend themselves to a complete and detailed presentation of your IT infrastructure and security controls.

Nonetheless, insurance providers need a thorough, unbiased report on the condition of your business –and, ultimately, it is your responsibility to present this risk profile to the insurer. This is absolutely something which your broker can and should be helping you finesse. The narrative beyond an application form may well be what resonates the most with insurers, particularly if your business is in a more challenging sector with constraint to available capacity.

Organisations need to know how the disruption of their business operations will, in turn, affect revenue and other related costs (for example, overtime, expedited freight costs, etc). If your organisation has a clear understanding of how the business will react in a cyber crisis and how business interruption loss will be adjusted and covered under the policy, then generally you can avoid wasting time, energy and money.

Know your partners

No organisation is able to handle a ransomware attack, much less an insurance claim, entirely on its own. Indeed, your organisation's knowledge of (and collaboration with) your various vendors and other business partners is going to comprise a critical aspect of the preparation and recovery processes.

Who are you going to call when something happens, and when will you call them? What happens if you notify the ICO too early? What legal and financial considerations should be considered prior to paying a ransomware demand? What are the implications if you use vendors that are not approved by the insurers? What happens if you notify your insurers two weeks into the remediation? Who can you count on to understand your situation and aid in your recovery? Needless to say, you do not have time to formulate a plan in the moments following an attack. You need to know who your trusted partners are, and you need to have agreements already in place before an incident occurs.

The process of preparing your partners begins with an equally critical question: Is your house in order? Are you ready for someone to come in and help you get back on track in the event of a cyberattack? To borrow an aviation analogy: Once you've secured your own oxygen mask, you can then begin to assist others. After all, when you think about it: only once you're in a position to accept help does it make sense to ask for that help.

When working with your insurer to identify those vendors that will be working with you in the event of an incident, make sure you have considered all your options as they relate to your business, including asking questions such as:

- Have you approved your vendors?
- Have you vetted them thoroughly?
- Are you comfortable with their rates?
- Are you going to use the insurance panel, or your own preferred vendors?
- Will insurers approve the use of your preferred vendors?
- Have your preferred vendors completed preliminary conflict checks to confirm that they can act for you in the event of an incident?

Testing your plan

In cyber security, not only is it important to test your security protocols to mitigate the chances of suffering a cyberattack in the first place, but it is also vital to test your incident response plan. Sophisticated testing is preferable – the more parties that participate in the testing the better, obviously – but even unsophisticated testing is better than nothing. Even a one-day exercise in which you walk through a semi-realistic attack with employees and your preferred vendors can be tremendously valuable in the long run.

In testing your plan, the vendor management aspect is particularly important, because you want to simulate a real-life incident with a natural response and a genuine claims process that mimics what will actually take place. With this in mind, you want to make sure the process is clear. You need to know exactly who is going to do what, who is going to contact whom, whether your backups are accurately configured and secured, and whether each party knows what to do in the event of several potential scenarios.

The chain of command for who brings in vendors, and how and when this is done, is critical to reducing the time between a breach and an organisation receiving the expert vendor support it needs – a factor that is tied closely to the overall cost of the claim. In S-RM's study, two of the most common contributors to higher costs in the incidents analysed were a lack of swift engagement between the board and expert vendors, and breakdowns in communication between the executive decision makers and technical teams. The common thread to both factors was the leadership teams' lack of prior awareness of the critical decision-making processes in advance of an incident that should typically be addressed in even an entry-level test of an organisation's incident response plan.

Don’t prejudice your chances of recovery

When working alongside insurers to plan for a potential cyberattack, organisational leaders need to make sure that they do not do anything to prejudice their chances of recovering their losses from the policy.

If you have completed your preparation (including practising your incident response plan) and if you’re talking through potential issues proactively with your vendors and your insurance company, then you essentially should know what steps need to be taken. In turn, you should know how the insurer is going to respond, leading to a process that goes smoothly and efficiently. By adopting this approach, it may be possible to identify how and where interim payments on account could be made in an effort to minimise the overall impact on cashflows. Furthermore, this type of preparation should also assist in ensuring that the final claim is settled on a timely basis, thereby allowing senior management to get on with running the business.

The importance of the initial reaction

The mindset you need immediately following an attack is to be ready for anything. And, truthfully, if you have done the required preparation in all its various forms, then you should be ready for anything. At the moment an incident occurs, your degree of risk preparation boils down to your organisation’s answers to these questions:

- What have you previously done to plan for specific scenarios?
- What operational IT infrastructure do you have, if any?
- In the event of an incident, what are you ready to do? What are you not ready to do?
- What situations have you prepared your vendors for, and are they ready to respond?

These questions are simply a starting point, of course. An incident response plan cannot account for every possibility. However, robust planning (and asking the proper questions throughout the process) can serve to guide your organisation’s plan in the optimal direction. The answers to the above questions should provide a window into how your plan needs to be adjusted in the event of different scenarios. And naturally any changes to your plan should be documented and clearly communicated to all relevant stakeholders.

Competency of your IT team

At the point of an attack, the competency of your IT team is a huge factor in being able to successfully respond and recover. S-RM’s study suggested that it actually might be the biggest factor. It is a component that is often overlooked by organisations that are so consumed with technology, insurance and other factors that they lose sight of the actual human beings who play such a critical role in the process.

The competency of your IT team goes well beyond the head of your team. In the event of an incident, significant levels of support will be needed from all members of the IT team. In fact, it likely will require the full IT team to assess the scene, repair the damage and prevent any further disruption, even with the support of outside technical vendors specialised in rapid network restoration and recovery.

Of course, it is not necessarily easy to assess an IT department's potential level of competency to handle a significant cyber incident. But you can begin by asking questions such as:

- Have they handled a ransomware event before?
- If so, how serious was that incident and what was their role within that team?
- Are they bright, technical and detail-oriented?
- Do they know what to do and, just as importantly, what not to do?

If there is a good network map and a detailed register of the IT equipment and applications that are operated across the organisation, as well as well-written and tested policies and procedures, that is typically a sign of a competent IT team. Needless to say, in the immediate aftermath of an incident, you are going to benefit immensely from having a strong team of IT professionals on your side.

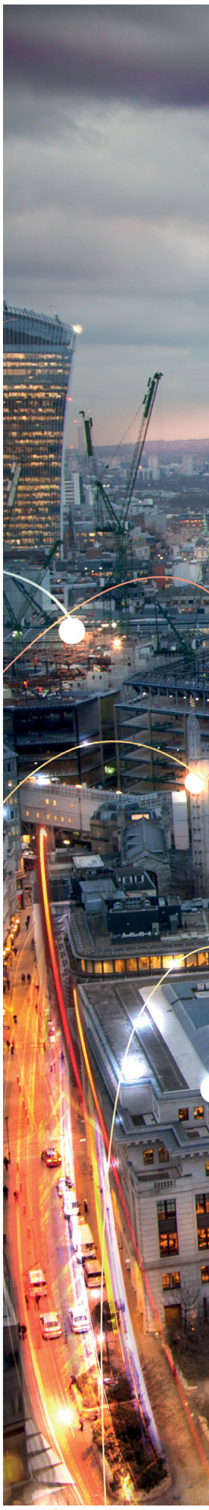
In general, a team that will be able to help you recover quickly and safely from a cyber crisis will exhibit the following traits:

- **Judgement**: An IT team which has the judgement to take quick action to contain the spread of an incident can make all the difference. In the early hours of an incident, a strong IT team could identify a ransomware outbreak in progress, quickly disconnect connectivity between sites and reset passwords, limiting the impact of an outbreak. The same team might immediately take action to protect backups at risk, securing a one-week recovery versus one that takes months. In contrast, a team with poor judgement might shut down servers mid-encryption, permanently corrupting data and destroying it forever, all the while leaving internet access open to a threat actor who takes the opportunity to delete backups before an expert vendor is even engaged.

- **Knowledge of the network:** An incumbent IT team that can deliver a clear and comprehensive picture of the organisation's network to outside experts, whether verbally or in pre-existing well-constructed documentation, will be able to turbo-charge the recovery from an attack. An outside vendor coming in fresh to an incident has a steep learning curve to get to grips with a new network. There are no magic solutions to transferring that knowledge over: either the incumbent IT team has a good understanding of the organisation's own network and will be able to share that information in the space of hours, or it might take days for outside technical support to reverse engineer an understanding of the network before it can begin helping effectively. When the IT team has a good handle on things, a technical incident response vendor will be able to collect evidence, deploy security software and help you rebuild after an attack exponentially quicker.

- **Collaboration and communication:** IT teams that are responsive and can quickly overcome any defensiveness or panic to collaborate with outside technical vendors will ensure your recovery is efficient and critical evidence is preserved. Too often, it's a legacy server or system that no one talks about that is the key to identifying how an attacker got in, which could have been raised to outside experts on the first call and removed from the network. Too often, IT teams put their heads down and try and recover systems on their own without engaging with outside experts, leading to insecure recoveries and duplication of work down the line. The best IT teams will be partners with outside experts, working alongside them to get the practicalities of the response done. They will be open and clear in communicating the state of the network and understanding that everyone is there to fulfil the same goal – resolving the incident as quickly as possible.

You are not expected to have all the expertise or resources you need in house to deal with it. Leaning on your experienced vendors for expertise and extra hands is unavoidable. However, your IT team's competence will greatly impact the effectiveness of the response.



02 PREPARING FOR A POTENTIAL ATTACK

03 What to do moving forward

As the underwriting and claims process is a partnership between the policy holder and the insurer, there are certain steps you can take moving forward to strengthen this relationship. Of course, the success of this relationship – like virtually everything we have talked about – comes down to preparation and communication.

Whether it is working through various scenarios in advance or talking with the insurer about the policy language, the importance of preparation and communication as you move forward in your relationship with your insurance company is paramount. It is simply never too late to commit to these critical concepts.

After all, you do not want to end up in a position where a claim goes poorly and you need to redo some or all of the planning process. You certainly do not want to have to change insurance companies or other vendors well after the fact. Changing insurers and/or vendors can result in the time and cost previously spent having to be repeated as part of bedding in these new partners. There is a significant cost associated with changing your mind.

So as noted earlier, you want to make sure you move forward knowing everything about your insurance company and insurance policy, not to mention your other vendors and of course your own organisation. Remember everything you learned from your incident response planning. Use what you learned and then observe the results to determine what steps can be taken to improve the overall claims process moving forward.

Looking ahead

When it comes to preparing for a potential cyber incident, Mike Tyson may have said it best, believe it or not: “Everybody has a plan until they get punched in the mouth.”

In short, you do not want to be caught unprepared. In the immediate aftermath of a ransomware attack, you do not want to realise that your team is short-handed or that you are not on the same page with the insurer, or that you have not looped in other key vendors. You do not want anyone in the supply chain to be unsure of what to do, and you certainly do not want your employees to be in a position where they do not know what to do after an attack. To put it simply, you do not want any surprises.

With that in mind, we are leaving you a checklist featuring 10 tips – most of which tie back into planning and/or communication – that you may want to consider moving forward as you look to avoid these expensive, time-consuming pitfalls before, during and after a cyberattack.

Checklist

1 Ensure your response plan defines roles and responsibilities for both internal stakeholders and external vendors in the event of a cyber crisis.

2 Ensure you thoroughly onboard the key external IT, legal, PR and accounting vendors you would use in a crisis and make sure this happens at the insurance policy bind stage. If possible, arrange an all-hands face-to-face meeting, and confirm commercial rates, review contracts and share relevant technical information at this point. Don't leave it until you have an incident.

3 Prepare a detailed understanding of your network infrastructure, including asset inventories and diagrams, and make sure you keep periodically updated copies stored offline. Plan ahead of time for how you would give an external technical team access to your infrastructure to help in the event of an incident.

4 Map which applications and systems are most critical to revenue generation and share this with your insurance provider and your nominated response experts.

5 Walk through your plan and rehearse common threat scenarios regularly.

6 Make sure to update your plans and rerun incident simulations when your circumstances change, such as after a large acquisition, following a significant change in your infrastructure or after departures/onboarding of key executive management personnel.

7 Ensure you understand your policy response and coverage in detail. Engage with your broker and carrier if you are unsure, and make sure you know their processes in the event of a claim.

8 Review the competencies of your incumbent IT team to support a response to a cyber crisis. If there are gaps in their capabilities, engage external support to train them on major threat scenarios and build in the right redundancy for a rapid recovery in the worst-case scenario.

9 Ensure that you have modelled the financial consequences of an incident and compared all the economic losses to both the total sum insured and the policy wording to identify where there may be any gaps in coverage. If gaps are identified, work with your broker and insurer to establish whether these can be addressed pre-bind.

10 Once incident simulations have identified the expected nature of operational disruption and the timescale for partial and full reinstatement, for each key client, develop an action plan on how that relationship is to be managed in the post-incident period, both from a communications standpoint and with respect to specific actions that can be taken to minimise disruption at the client.

airmic

Marlow House
1a Lloyd’s Avenue
London
EC3N 3AA
+44 207 680 3088
enquiries@airmic.com
www.airmic.com