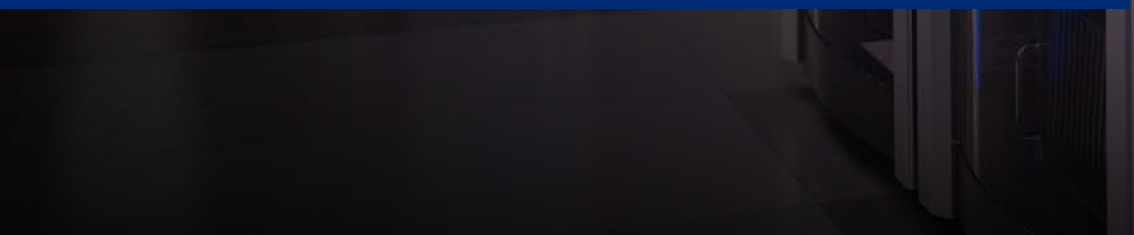
Marsh

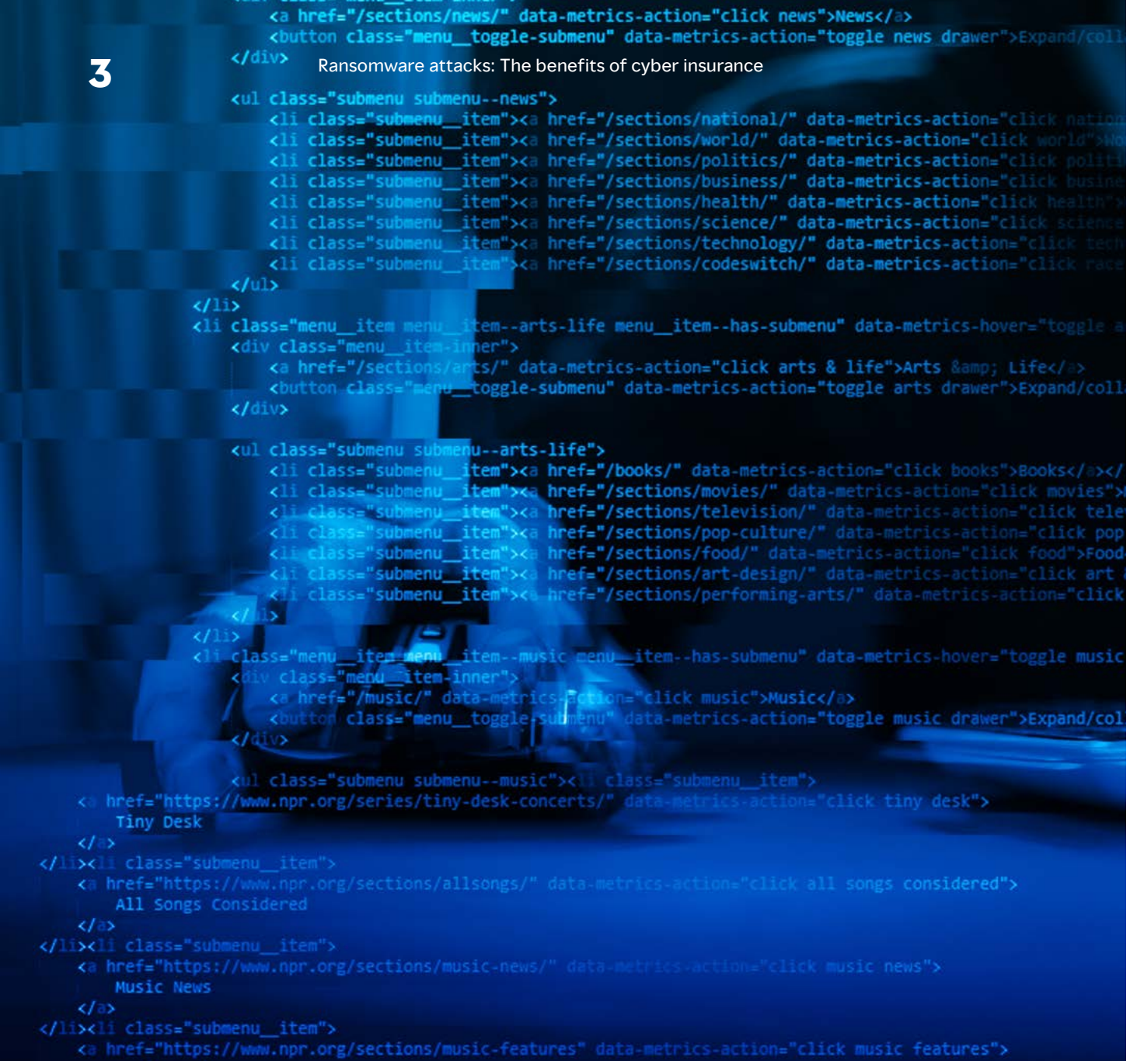
Marsh Specialty

It’s not all about the ransom: Benefits of cyber insurance



The threat of ransomware strikes has never been more prevalent, with the UK's National Cyber Security Centre (NCSC) reporting that it responded to more than three times as many events in 2019-2020, compared with the previous year. No business, whatever its type or size, appears to be completely immune from the threat of ransomware incidents.

In the event of a ransomware attack, cyber insurance provides assistance from specialists on containing a breach, navigating the demands of the cybercriminals, and with the subsequent decryption of data. A policy can also cover the business interruption and expense of restoring data systems, which are often the biggest financial impacts of a ransomware strike for organisations.



The price of refusing to negotiate

Many organisations affected by a ransomware strike instinctively balk at the idea of engaging with the attackers. Some businesses remain steadfast in this approach, even when there is no other means to recover their data, such as by using offline backups, and the outcome could be costly.

In one notable case, the US city of Atlanta in 2018 reportedly refused to authorise a US$51,000 ransom and consequently spent US$2.7 million on external consultants to remediate its systems, with the total recovery costs rising to US$9.5 million. In many cases, the extortion amount itself is a minor proportion of the overall cost to the victim. In May, Ireland's Health Service Executive (HSE) suffered an attack, which the organisation said would cost at least €100 million, despite the original ransom demand rejected by HSE being just under €16.4 million.

> **The largest financial impact for targets of ransomware is not the ransom itself, but rather business interruption and data restoration costs.**

The real cost of ransomware

Business Interruption and Data Restoration

The largest financial impact for targets of ransomware is not the ransom itself, but rather business interruption and data restoration costs. Even when a ransom is paid, and the data is successfully decrypted, it can be a number of weeks before the affected systems are fully operational again. The average downtime following a ransomware attack in Q1 2021 was 23 days, according to ransomware experts Coveware.

During this downtime period, the business experiences not only reduced turnover and sales, but also increased costs of working, as it must incur temporary workarounds in order to keep operations running. These can include the installation of new outsourced servers.

If an organisation decides not to authorise a ransom, there will be additional costs to rebuild or replace systems and data. These may have to be recreated from scratch if there is no up-to-date uninfected backup.

The Scottish Environmental Protection Agency, for instance, refused to negotiate when it was attacked in January 2021 and has since advised that its systems may not be restored fully until 2022. Meanwhile, HSE's chief executive said in June hospitals may remain affected for six months, despite the organisation receiving a decryptor key without having to resort to paying its attacker, the Conti ransomware group.

Indeed, the impact to a victim may continue for some time, even if the ransom is paid. The chief executive of Colonial Pipeline, which paid a US$4.4 million ransom following May's attack by the ransomware group DarkSide, said the company needed "months to recover some of its business systems" and that the final cost of the restoration is expected to be "tens of millions of dollars".

Well-designed cyber insurance programmes will cover such business interruption and data restoration costs, up to the date when the systems are fully back up and running. Payment of a ransom is a decision for the insured, not insurers, and cover does not depend on a policyholder's decision on whether or not to engage with the attacker.

Perhaps the best-known example of an insured that refused to negotiate with an attacker, but nonetheless successfully made recoveries from its cyber policy, is the aluminium producer Norsk Hydro. The company's 35,000 employees worldwide were reduced to using pen and paper, when 22,000 computers across 170 sites and 40 countries were infected with ransomware.

> **Well-designed cyber insurance programmes will cover business interruption and data restoration costs, up to the date when the systems are fully back up and running.**

Crisis assistance from specialist vendors

While a CEO may be worried by a drop in profits in the midst of an ongoing ransomware incident, their most immediate concern will be how to contain and remediate the breach as quickly as possible. This urgency is often compounded by both a lack of clear facts when the attack starts, and the unfamiliarity of the business's internal teams with such an aggressive intrusion. Even organisations that have developed cyber incident playbooks can find they are ill-prepared to respond when the threat actor, faced with non-payment of the ransom, escalates the situation.

This is precisely where cyber insurance can step in and provide crucial support to companies that might otherwise be overcome with paralysis. A policyholder will have access to an array of specialist vendors, who are experienced in handling different types of ransomware attacks and other cyber incidents every day.

These experts will be best placed to help stop the spread of the virus and safely rebuild the affected systems, assist the policyholder in fulfilling any notification obligations, deliver customer support, and defend legal claims. Where the ransom is not met, assistance from the vendors available may become even more crucial. Vendors available under a cyber insurance policy are enlarged upon the categories on the following pages.

IT incident response consultants

These are specialists in containing a breach. They also perform a forensic investigation to establish the cyber kill chain – the series of events of a cyberattack – including the initial attack vector, how the virus spread, and what personal and other confidential data is affected. Having responded to countless similar incidents, such experts are skilled in ascertaining the full extent of the damage caused by the particular ransomware strain deployed, and in assessing the most secure means to bring the policyholder's systems back online without falling prey to the same vulnerability.

Sometimes, computer security experts independently have access to a proven decryptor key for the strain in question, and will be able to restore the data without using backups. If so, they will check for any malware persistence, such as backdoors planted by the threat actor. They can install endpoint detection and response (EDR) and other solutions to actively monitor and guard against the reinfection of the network, which could remain at risk even following restoration from a backup.

In addition, security consultants can assist should a threat actor ratchet up the pressure, when a victim refuses to pay. In the first quarter of this year, 77% of ransomware attacks included a threat to leak exfiltrated data, according to Coveware. Expert vendors can evaluate this "double extortion" risk, by determining what data has been stolen, as well as giving their insight into the particular threat actor's past tactics and current activity on the dark web. Similarly, they will assist in repelling any distributed denial-of-service (DDoS) attacks, which some hackers threaten to launch, if they are ignored.

Legal advisors or "breach response counsel"

These are lawyers who specialise in data privacy. They are able to advise the policyholder on how to fulfil any legal obligations that could arise from the incident in light of legislation, such as the EU's General Data Protection Regulation (GDPR), and the UK's Data Protection Act 2018. Responsibilities may include notifying the relevant data protection authority, such as the Information Commissioner's Office (ICO) in the UK, and the Data Protection Commissioner (DPC) in Ireland. Other relevant regulators the policyholder may be subject to, as well as affected individuals, may need to be notified. These legal advisors can provide advice in the event of a regulatory investigation.

Breach response counsel are proficient in establishing and assessing the data that has been compromised, in order to advise the policyholder, on whether it is necessary to make a breach notification. This may be necessary, even if the threat actor has not accessed any personal data. At the beginning of the year, the European Data Protection Board, comprising representatives from all the data protection authorities in the EU, outlined scenarios where, even if the ransomware victim has adequate backups and no exfiltration of personal data has occurred, affected individuals may still be at high risk and therefore should be notified.

If the attacker is threatening to disclose exfiltrated data, breach response counsel can advise the policyholder on the legal avenues available to prevent publication, such as injunctions and takedown notices. Counsel will also advise on how to minimise the risk of third party claims being brought, including by protecting internal and vendor reports and communications with legal privilege, where possible.

In the event of litigation, cyber insurance offers access to privacy lawyers to defend claims. While settlements and judgment awards for data breach claims are relatively low, the cost of defending such claims can be high, in comparison. Total costs can soon mount up if a large number of individuals allege they have been affected and seek compensation. Last autumn, a number of the more than 125 UK organisations affected by the ransomware attack against the service provider Blackbaud, subsequently received group litigation claims by customers. Cyber insurance delivers the means to contest these types of claims, which are frequently brought, even when there is no concrete evidence of unauthorised access to personal data. The cover also funds damages and settlements where necessary.

Notification services and customer call centre providers

In the midst of a crisis, when systems are down, an organisation's resources will be stretched to the limit. Often, there is simply no spare capacity to draft and dispatch thousands of notification letters to affected individuals, all within tight regulatory timeframes. On top of this, the organisation may be unable to field the surge in calls from anxious customers, alarmed by media reports and the possibility of their personal data being leaked.

These service providers can swiftly produce, at scale, breach notification and FAQ documents and send these out by post or email to affected individuals, in accordance with the relevant regulation. They are also able to staff call centres to handle follow up communications, give identity protection guidance, log complaints, and talk through customer care options, such as credit monitoring. These services can be performed with oversight from breach response counsel to ensure that all FAQs and communications with affected individuals are made, and regularly updated, in a way that minimises the risk of litigation against the organisation.

Credit monitoring service providers

Cyber insurance also funds the provision of free credit monitoring and identity theft protection products to notified individuals for at least 12 months following an incident. This option has perhaps become more relevant recently, as ransomware incidents increasingly involve suspected exfiltration of personal data.

In addition to setting up fraud alerts with the major credit reference agencies, some vendors also offer dark web monitoring, to check for compromised credentials and individual account details for sale. This can give affected individuals peace of mind, reducing their potential distress and risk of financial harm. This, in turn, helps lower the risk of litigation against the policyholder and regain goodwill from customers.

PR consultants

When an organisation suffers a ransomware attack, established facts are thin and speculation is rife in the press and on social media. Rumours can quickly spread about the purported theft of personal data or ransom negotiations. These can spiral into a groundswell of critical customer sentiment, citing the organisation's breached security controls and handling of the incident. In pressing for payment of a ransom, some attackers have even contacted customers directly, warning them that their data might be released if the organisation does not take action.

All this can significantly damage the victim's brand — and hastily prepared public announcements and press releases can further inadvertently admit liability to third parties or encourage legal claims. A ransomware victim with a large client base needs to be nimble and adapt its messaging as the situation continuously evolves. Cyber insurance will fund the cost of PR consultants, who are experienced in active crisis management and liaising with breach response counsel, to ensure that internal and public messaging minimises the policyholder's litigation exposure.

Support beyond the ransom

Many companies may already have their own long-standing suppliers, such as external corporate counsel, or outsourced IT service providers. However, these are usually more general experts who may be untested when it comes to a significant data incident. If so, they may be ill-equipped to handle the unique and highly pressurised demands of a ransomware attack, which may well intensify dramatically if the victim refuses to negotiate. Even where experienced vendors are available, they may only come at a high cost.

Cyber insurance gives policyholders access to a broad range of dedicated experts, who are specifically skilled in responding to ransomware incidents. This assistance — as well as coverage for the business interruption and data restoration costs that normally comprise the greatest financial impact on the victim — makes cyber insurance a vital component in an organisation's defence against ransomware.

> **Cyber insurance gives policyholders access to dedicated experts who are specifically skilled in responding to ransomware incidents.**

For more information please visit marsh.com or speak to you usual Marsh Specialty representative.

Neal Pal
Senior Product Development Specialist, Marsh Specialty
+44 (0)7392 123 093
neal.pal@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk adviser. With over 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. Marsh is a wholly owned subsidiary of Marsh McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people.

With annual revenue over US$17 billion and 76,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market leading firms: Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @ MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.