

Cyber Liability Insurance Handbook

ENTER




Main menu



01 Cyber risk: what it means for your business



02 What is a cyber-attack? How does it happen?'



03 Why does your business need cyber insurance?



04 Case studies



05 Understanding the Risk Placement Services cyber solution



A photograph of two men in business suits sitting at a small table in a modern office setting. They are looking at a document together. The image has a warm, orange-toned overlay. The background shows a large window with a geometric pattern of light-colored frames.

01. Cyber risk: what it means for your business





Why your business should rise to the cyber security challenge

The cyber threat to US businesses is significant and continuously evolving with many becoming prime targets for global cyber criminals. With such a reliance on technology in order to be connected at all times and conduct work effectively, cyber risks have become a top-of-mind issue. Businesses can no longer rely on traditional insurance coverage in this space and must take a high-level, holistic approach to how they develop their operations to promote a cyber-resilient culture.

Businesses are continuously looking to any margin improving efficiency. This often means the solutions are heavily reliant on technology and digital integration. As a result any loss of internet connectivity will have a significant impact on business operation.

According to Juniper's 2018 research study¹, small businesses made up 13% of the entire cyber security market in 2018, and yet surprisingly small businesses invest less than \$500 per year in cyber security products making them an attractive target to cybercriminals.

As we have just observed, with this online dependency comes sizable risk. So much so that, according to a report by Ernst & Young², smaller organizations are set to increase their cyber security budgets by 50% this year and 66% next year.

While an enhanced understanding of the cyber risk landscape has prompted organizations to spend more on their IT security, actual take-up of cyber policies still remains relatively low, with still 55% of companies not making 'protecting' part of their strategy.¹

Those companies operating in the financial/professional services sector have been the most active when it comes to the uptake of cyber insurance. They naturally host some of the world's most sensitive data, making it extremely attractive and the obvious choice for cyber criminals to target.

However, with the management of data and dependency on technology often a secondary concern for the majority of businesses, the benefit of a cyber policy in helping a business respond to, and recover from, an attack or data breach could prove to be invaluable and must not be ignored.

1. <https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats-2018>

2. EY Global Information Security Survey 2018-2019.





Cyber insurance explained

Key statistics to show why the threat of cyber cannot be ignored:



Ransomware business attacks in 2019 rose 365% from 2018.³



Only 10% of cybercrimes are reported in the US each year.⁴



Ransomware claims a new victim every 14 seconds.³



Ransomware payments topped \$11.5 billion in 2019.³



There were 204 million ransomware attacks alone in 2019.³



Ransomware downtime costs an average of \$8,500/hour.³

³ <http://www.itondemand.com>

⁴ <http://www.cpomagazine.com>



02. What is a cyber attack?
How does it happen?





What is a cyber attack? How does it happen?

Most cyber attacks or social engineering scams start with a single or series of “Phishing” emails. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.



1 in every 99 emails is a phishing attack. In a 5 day work week, this amounts to 4.8 phishing emails per employee.⁵



Phishing attacks increased by 65% in 2018.⁵



Approximately 14.5 billion spam emails are sent every day.⁶

According to Proofpoint’s Human Factor report, 76% of businesses reported being a victim of a phishing attack in 2018.⁵

Phishing is on the rise, and hackers now target the vast majority of businesses, regardless of size. What’s more, average users are not spared either, receiving a growing amount of spam mail each week.

These emails masquerade as legitimate emails and often point to a need for immediate attention. Common phishing emails and attempts at impersonation fraud include the CEO email scam and emails purporting to be from respectable companies/ organizations such as Apple, Amazon, various mobile phone networks, highlighting spurious orders and calling for action to stop these transactions.


Hackers know that the weak spot within any organization is their employees and take advantage of this by sending phishing and spear phishing attacks that are difficult for employees to identify as a threat.

5. <https://www.proofpoint.com/us/human-factor-2018>

6. <https://www.symantec.com/security-center/threat-report>

7. Avanan infographic



A close-up photograph of a hand holding a white pen, poised to write on a document. The document features a table with columns and rows, and some handwritten text. The entire image is overlaid with a semi-transparent green filter. The background is blurred, showing another hand and more documents.

03. Why does your business
need cyber insurance?





Why does your business need cyber insurance?

Many organizations assume that their exposure to risk is limited, and ask themselves “why would someone hack me?”

Any business that relies on computer systems to generate or store business-critical information can have a very real exposure to cyber risks if they lose or are unable to access their digital files. In addition to the operational challenges that such a loss of data or interruption may cause to trading, the biggest concern is consumer trust. Imagine an online retailer who was a victim of a hack or significant data breach. The key risk is not only the lost business and the costs incurred to remedy the breach, but the loss of customer confidence and lasting reputational harm.





Your business could be at serious risk

Good cyber coverage does not just stop with incidents involving electronic or online interference – it should also protect your communications more broadly to include areas like private data and communications, in all the formats you use, electronic or otherwise.

Answering ‘yes’ to any or all of these questions means a cyber-insurance policy should be in place.

Just ask yourself:

- Do we hold sensitive customer data, such as names, addresses, banking information or other confidential records?
- Are we reliant on computer systems and/or email and the internet to conduct business?
- Do we have a website that’s a store front, sales or support desk for our customers?
- Do we operate under a payment card industry (PCI) merchant services agreement?





If you already have cyber insurance - do you really know what you're covered for?

Many insurance policies include an element of cyber insurance, but it can be difficult to get to grips with exactly what protection you have. You might not be aware of all the ways in which your business is vulnerable, or may not be used to cyber-related jargon within your policy or in the media. This makes it hard to compare your policy to what you need – especially because there is little commonality between one insurance policy and another.

Your Cyber Insurance policy alone is not enough

Not all risks can be insured, and, as a rule, prevention is better than cure, so your insurance should be seen as just one part of the risk management equation. An effective strategy requires an understanding of the specific risks to which you're exposed, the capabilities of your organization's security systems and an appropriate combination of measures to manage the risks.




04. Case studies





Case studies & sector examples

Below are example scenarios which have left the organizations with significant financial and reputational consequences.


CLICK ON A CASE STUDY





Finance




Non-Profit Organization




Public School District



Manufacturing




Public Entity




Healthcare




Retail




Cyberterrorism




Employee information compromised



Ransomware



Trademark



Case Studies



Finance

Compromised email system of a wealth management advisor led to phishing emails being sent to customers.

Hackers were able to infiltrate the email system and create false invoices appearing to come from the wealth management advisor's email account. The payment instructions were altered to divert payment to the fraudster's account.

Coverage was provided under the incident response insuring agreement to provide for legal advice and forensics assistance to determine the cause and extent of the breach. The incident was discovered fast enough to avert monies being paid, but the unauthorized access to the wealth advisor's network triggered the state privacy law's requirement to notify those whose personal information had been viewed. Costs for the notification and credit monitoring were covered under the policy as well.



Non-Profit Organization

The insured terminated an employee who then downloaded donor files to a thumb drive and then deleted them from the insured's computer system.

The insured is in contact with Legal Counsel to determine if notification is required. There will be legal fees and possible notification costs that would be covered under the policy.

Disgruntled employees are one of the leading causes of Cyber Breach incidents. From downloading and selling customer lists and financial information to providing accessibility to password-protected systems, the financial ramifications to non-profit organizations, without a Cyber Liability Policy can be disastrous.





Public School District

Hackers were able to force their way into the school's accounting system resulting in employees' payroll checks being deposited into a fraudulent account.

The costs associated with this claim were for Data Breach & Crisis Management. There was an investigation of the insured's computer system to be certain notifications were not needed.

While the payroll checks were immediately voided without loss of funds, the cost of this breach included payments made for Computer Forensics and Privacy Counsel. Total paid was \$65,000.



Manufacturing

Fraudulent wire instructions were sent to the insured's client by hackers who were able to disguise themselves as the manufacturing company.

They took over an email account and provided a different bank routing number and account information to the customer. The company sent the payment to the hacker's overseas account.

This is an example of "Phishing" and monies paid to the hackers would be covered under a Cyber Liability Policy with this endorsement. Most times the wire transfers are untraceable and the wired money is never recovered.





Public Entity

The city's finance manager discovered ransomware on the city's servers.

The servers contained accounting software, personal employee information and payroll data. The hacker's message stated that "bitcoin ransom would be negotiated on how quickly the city responded". A third-party IT forensic team, contracted through the insurance carrier, negotiated the ransom payment amount from \$1.5m down to \$776k and investigated the business's system for data access or exfiltration. The claim payment exceeded \$1m.

The knowledge needed to negotiate, pay and then protect the computer systems from further damage is beyond the grasp of most city employees. The purchase of a Cyber Liability policy provided the city with a team of Cyber experts to help with all aspects of this data breach.



Healthcare

A non-encrypted laptop, that contained Protected Health Information, (PHI), was stolen from a Doctor's office.

HIPAA notifications. HIPAA notifications were made to the affected patients and a forensic investigation is underway regarding the security of the network and whether the 2,500 individuals whose information was compromised are at risk for identity theft.

"Out of Pocket" payments for this Doctor's office who did not have a Cyber Liability policy, included \$21,000 for Breach Counsel and notification costs as well as ongoing costs for Computer Forensics and possible HIPAA fines and penalties that could be assessed \$1.5 Million.





Retail

A furniture store experienced a wire fraud loss of \$47,630.

Spoofed emails were sent from an email address that appeared to be from a trusted purchasing agent. The funds were sent by the office manager. Several days later, after a phone call, the office manager learned that the instructions were false. The firm notified the bank and tried to stop the payment.

“Social Engineering” is quickly becoming one of the most prevalent cyber-crimes. Many Cyber Liability carriers now offer Social Engineering as an endorsement or as a First-Party coverage on their form.



Cyberterrorism

A client’s Twitter feed was hacked and used to broadcast pro-ISIS propaganda.

The client immediately called the hotline, and based on their advice, was able to identify how the hacker had got in and compromised the Twitter page. As a result, forensic experts were able to identify the weak link.

However, two weeks later, the hackers struck again. This time, a team of cyber forensic specialists were sent in to restore the security of the client’s website, email system and Twitter to prevent a recurrence.

The cost to the insurer was \$235,000, a cost that without cyber insurance would have been carried by the client.





Employee information compromised

Specific incidents demonstrate the added value of a breach response team and the resources that can be brought to support an insured.

The insured became aware that a number of its employees were being subjected to tax fraud – tax refunds had already been secured in their names. Supported by our breach response team and external forensic teams, the insured confirmed their systems were secure and the cause was likely an external provider.

The breach response team provided notification advice and credit monitoring services to the affected employees, with each receiving credit protection for one year.



Ransomware

Ransomware is pervasive and easy to introduce into systems, making it a common claim.

An insured's employee clicked on a malicious link which resulted in the download of CryptoLocker ransomware - malware that encrypts the system it attacks and demands payment to release.

Assisted by the breach response team and external forensic teams, the insured's internal team was able to restore elements of the compromised data, but the issue resulted in paying over \$550,000 in extortion payments using a cryptocurrency.



Trademark

Our insured was sued for trademark infringement, regarding a trading name they used.

Cover was granted under the media liability coverage and lawyers were instructed to defend the litigation, which was settled prior to court. The program covered all costs after the policy retention.



A grayscale photograph of a woman with curly hair, smiling as she looks at her smartphone. She is wearing a dark top and a light-colored cardigan. The background is blurred, showing what appears to be an outdoor setting with other people.

05. Understanding the
Risk Placement Services
cyber solution



Understanding the Risk Placement Services cyber solution

Key benefits

You'll have access to a 24/7 breach response hotline, meaning you'll be speaking to a specialist within minutes to help get your business back up and running as quickly as possible. The specialist will guide you through the process and give you appropriate advice as and when you need it.

- ✓ Policy tailoring and consultation available
- ✓ Covers private data and communications in many different formats – paper, digital or otherwise
- ✓ Also provides extensions to coverage including reputational harm and cybercrime.



Working out your needs

Use our cyber business check-up and policy overview to determine the level and type of cover your business needs.

[VIEW DETAILS](#)



What does our solution cover?

Section A: Cyber Liability + Incident Response
Section B: Cyber Business Interruption
Section C: Cybercrime

[VIEW DETAILS](#)



Cyber business check-up

Risk	Exposure	Yes	No
Loss or theft of customer information from organization's systems.	Do you keep customer or employee information electronically?	Yes	No
	Are customer credit card or bank details kept on your systems?	Yes	No
	Are these details encrypted?	Yes	No
	Do you have an IT policy in place regarding the handling of this type of data?	Yes	No
	Do you have a stable finance team?	Yes	No
	Do you update security software as soon as advised?	Yes	No
	Do you have a privacy policy in place governing your collection of private data?	Yes	No
	Are there automated checks and audit trails built into the financial systems?	Yes	No
	Do new supplier bank details need FD approval?	Yes	No
	Are checks made monthly on funds leaving the organization's account?	Yes	No
Are there flags set to highlight where and when information leaves the system?	Yes	No	
Cyber Extortion via Ransomware	Are you reliant on your network and critical business data being accessible in order to operate your business?	Yes	No
	Do you backup your critical data or does someone do it on your behalf?	Yes	No
	Is your backup segregated from your primary network via firewall or by some other secure means, so that an intrusion into your network doesn't provide a pathway to your backups?	Yes	No
	Do you have backup redundancies in place ie: backups are stored in the cloud and your a secondary source from which to restore your data?	Yes	No
	Do you regularly test your backups to ensure the data isn't corrupted and can be restored?	Yes	No
Do you regularly train employees regarding what to do and whom to call in the event of a ransomware incident?	Yes	No	
Denial of service attacks on websites – resulting in you being unable to collect payments, issue sales invoices, or just provide information to your customers, employees or suppliers.	Do you operate a website that provides you with an income or provides your customers with assistance?	Yes	No
	Are you PCI compliant?	Yes	No
	Do you have someone monitoring your website for attacks?	Yes	No
	Do you have a process in place if your website is attacked but the attack is not successful?	Yes	No
	Do you have a process in place if your website is successfully attacked/corrupted?	Yes	No
	Have you discussed what to do with your Internet Service Provider?	Yes	No
	Have you discussed what to do with the police?	Yes	No
	Is there an established recovery process?	Yes	No
Has the recovery process been successfully triggered before?	Yes	No	
Loss of customer data by Third-party suppliers/partners – whether by human error or deliberate act and the release of personal information relating to your supporters.	Do you permit data to leave your system?	Yes	No
	Do you have a contract with a third party that clearly defines what they can and cannot do with your data?	Yes	No
	Do you conduct due diligence to ensure that the contract is being complied with?	Yes	No
	Are you certain that third party staff are all trained on data protection?	Yes	No
	Are you certain that third party staff are all employed and not temporary in nature?	Yes	No

Whenever you have answered 'Yes' to the questions in orange you have an exposure. If you answered "No" to these questions, your exposure is significantly limited, so provided that you are confident of your answer you can move on and ignore the questions under that heading.

Whenever you have answered 'Yes' to the questions in blue, you have a control in place. However, if you answered 'No' there is a gap in your protection that should be addressed as quickly as possible.



What can Risk Placement Services Provide?*

The cyber insurance programs we place provide a range of cover in three sections; Cyber Liability and Incident Response, Cyber Business Interruption and Cybercrime.

Cyber Liability: Incident Response

Breach Response Costs

A data breach is the loss, theft or compromise of data. The cyber insurance we place is designed to cover costs such as notifying your affected customers; offering credit monitoring; setting up call centers for concerned customers; bringing in forensic teams to identify the reason for the data breach; and potentially removing the hacker – or the virus/malware – from your systems.

Real-world event:

- The insured discovered that an unidentified third party had uploaded files to their system, which allowed them to corrupt the insured's information files.
- Data obtained included private, personally identifiable information, including credit card information.
- The third party made fraudulent charges on multiple accounts.
- The insured was required to notify the affected individuals. Given the discovery of the fraudulent charges, the insured offered affected individuals an opportunity to obtain credit monitoring.
- The insured also wanted to manage the breach in the media to demonstrate decisive, responsible action so a public relations expert was brought in to assist.

The costs related to all of the above were covered under the Breach Response Costs section of the policy.

Regulatory Defense Costs

These are the legal costs incurred to comply with any regulatory action taken against you following a data breach.

Real-world event:

- An insured healthcare provider misplaced multiple drives that contained protected health information (PHI) for over one million patients.
- It was unknown whether the drives were lost, stolen or destroyed. The insured was required to notify the affected individuals, as well as the State's Attorney General.
- The Attorney General opened an investigation into the incident and fined the insured healthcare provider for failing to protect the information.

Cover under this section paid for the legal fees incurred by the Insured in connection with responding to the investigation and inquires. It also provided coverage for assessed fines and penalties. (Fine and penalties are insurable where allowed by law.)

*These are brief product descriptions only. Refer to the policy for exclusions and full terms and conditions applicable.



Cyber Liability and Incident Response

Security and Privacy Liability

This covers your liability in the event you suffer a data breach and you find yourself sued by affected customers or employees. This includes theft or altering of data, virus or malware, denial of service and other loss of data from your systems.

Real-world event:

- An insured boutique retailer emailed a group of customers to promote a sale with special discounts.
- Intending to attach a copy of the flyer detailing the discounts, the insured instead attached a copy of a spreadsheet that contained a customer list, including customer names, addresses and credit card information.
- The insured was required to notify all affected customers of the error and offer credit monitoring. The costs for this were covered under the Breach Response Costs section of the policy.

Several of the affected individuals filed a lawsuit against the insured and cover for legal costs and indemnification was provided for the insured under the Security and Privacy Liability section of the policy.

Cyber Extortion/Ransomware

These are the costs you may incur should a hacker steal data from your systems and then demand a ransom to avoid leaking the information, or, to provide a decryption key to restore access to your system. The software tool the hacker uses in this case is called 'ransomware'.

Real-world event:

- A small healthcare clinic discovered that an unauthorized third party had gained remote access to a server that contained electronic medical records.
- The third party posted a message on the server stating that the files and all information on the server had been encrypted and could only be accessed with a decryption key that would be supplied if the insured made a ransom payment.

The insured worked with law enforcement and determined that the payment should be made. The \$550,000 payment was covered under the policy and the sum was reimbursed.



Cyber Liability and Incident Response

Multimedia Liability

This covers your liability in the event you are sued as a result of information provided within your website and social media channels – for example on your website, Twitter feed or Facebook page. Typical examples would be breach of copyright, libel or slander, plagiarism or defamation.

Real-world event:

- The insured began a blog to share information to customers and the public.
- The blog page contained a logo/image that was similar to a design that had been copyrighted by another party.
- The other party sent a ‘Cease & Desist’ letter to the insured demanding that they remove the image from the blog.

Discussions between the parties failed and the other party sued the insured. Costs were covered for breach of copyright under the Multimedia Insuring Clause in the policy.



Cyber Business Interruption

1. Cyber Business Interruption

Business interruption is the income a business can lose as a result of a network disruption to the insured's systems.

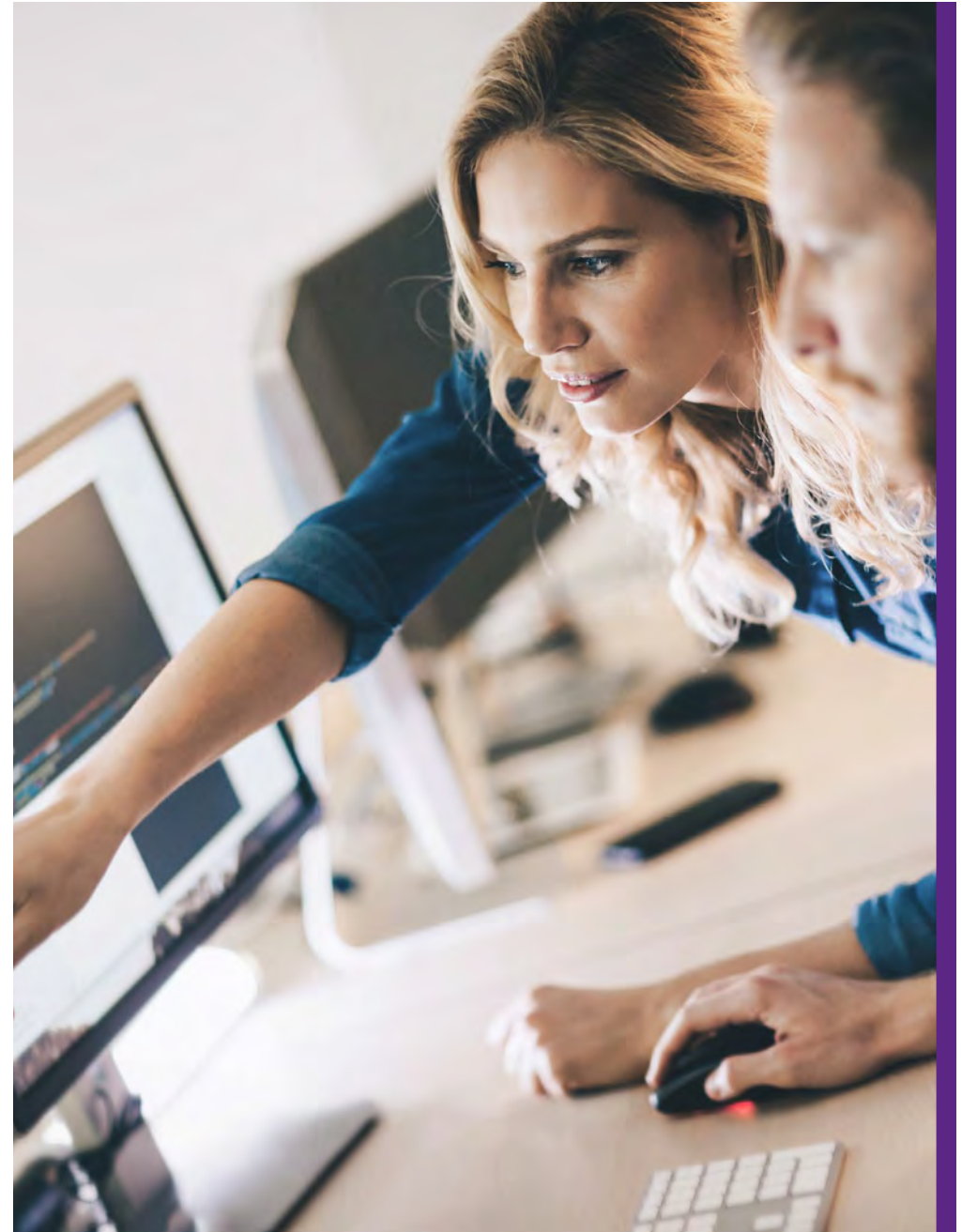
- Many companies now outsource business critical IT processes like card payment processing or data storage.
- Today's cyber policies should also provide coverage for dependent business interruption. This indemnifies the insured for loss of income due to a vendor, such as a payment processor, suffering a service outage due to security breach.
- Expansions of coverage can be provided to cover more than just business interruption due to a security breach. Discuss these options with your RPS broker.

2. Digital Asset Restoration

This covers the costs incurred by the insured to restore affected data after a breach event or if security is compromised.

3. Cyber Reputation Business Income Loss

This covers earnings loss due to the loss of current or future customers (usually within 12 months) from a data breach or network interruption event.



Cybercrime/Social Engineering

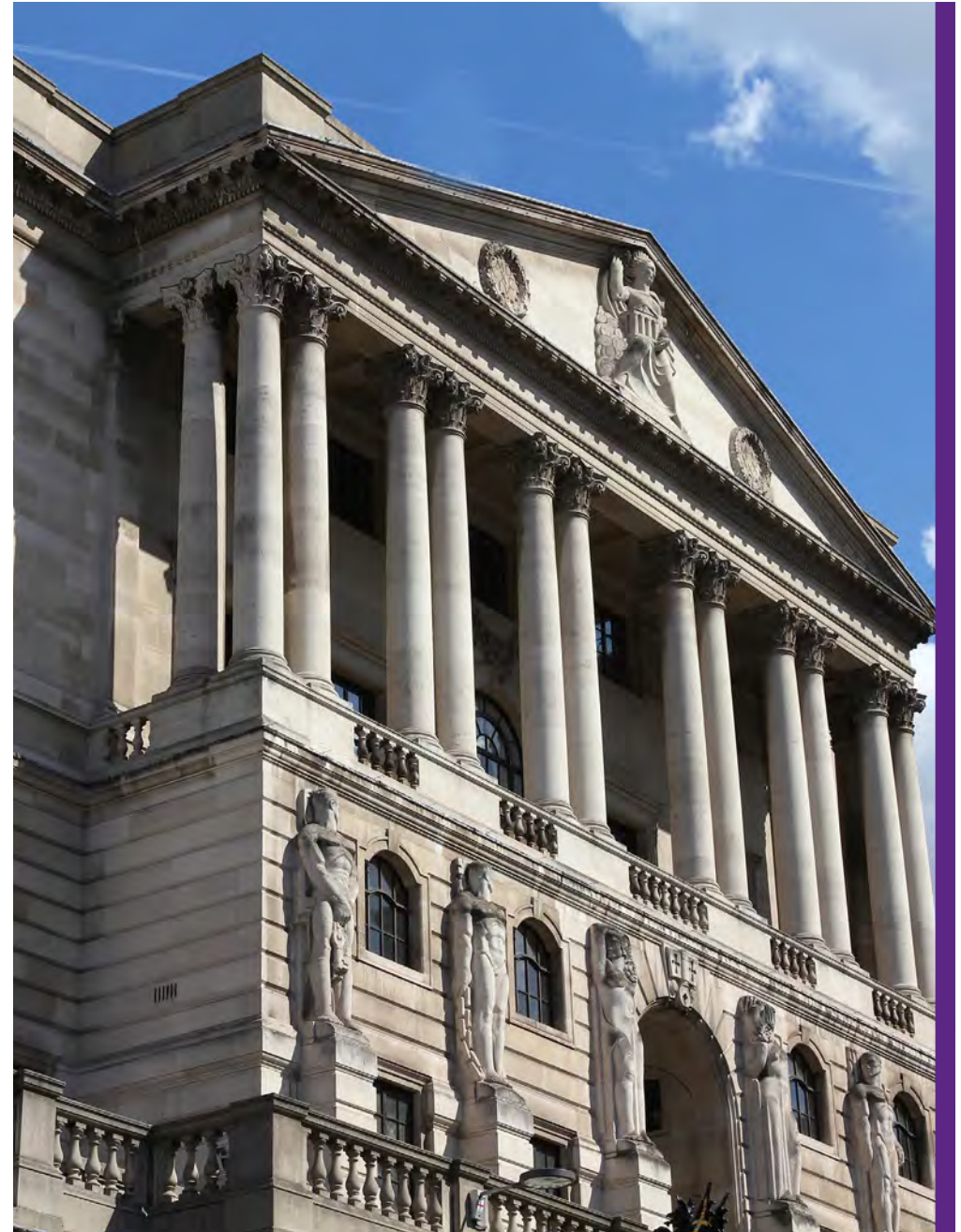
Coverage is provided for the theft of your funds or assets:

- Through the manipulation or misuse by a 3rd party of computer hardware, software programs or systems.
- As the result of the insured willfully transferring their money or goods to a third party based on a fraudulent instruction that is typically delivered electronically or via telephone. This type of crime is also known as 'social engineering fraud' or 'impersonation fraud'.

Real-world event:

- The accountant of a medium sized manufacturing company received multiple emails and calls in quick succession – including emails from what appeared to be the company CEO – telling them to transfer funds to various accounts for the acquisition of another company.
- Pressured into acting quickly, the accountant transferred the funds, costing the company thousands.

Insureds are encouraged to implement a set of checks and balances within their organization to prevent social engineering fraud. For instance, calling a prior known number of the person or entity requesting the transfer of funds to verify its authenticity before acting on the request. Simple call-back measures such as this can help prevent the vast majority of social engineering fraud losses.



If you would like further information or to discuss your cyber insurance needs in more detail, please get in touch with us today.

Contact your trusted RPS Broker for a quick quote or more information

