beazley

beazley security

Cyber Insurance Buyers Guide 2024

Winning the battle against cyber risks

What's included in this guide

Winning the battle against cyber risks

This guide helps you understand the cyber risk landscape and how to navigate it.

New technology and digital transformation brings a huge amount of unintended and unseen risks. IT networks, old legacy software and systems, cloud storage and platforms, connected devices and digital banking: the greater the investment in technology and change, the greater the cyber threats. It's a vicious cycle.

When a cyberattack hits, the costs can quickly spiral. There's handling the immediate breach, data investigation and recovery. And then a great deal to manage after the incident too – repairing brand damage, court costs, external consultant fees like IT security, PR, legal, and communications, as well as potential fines or penalties. Having all these necessary skills and expertise in-house or on retainer can be expensive, and traditional cyber insurance that reacts to an incident simply isn't enough anymore. But, it is possible to proactively manage down these threats and develop your cyber resilience by partnering with those who have the know-how in this field.

Why Beazley and Beazley Security?

The world of cyber threats doesn't have to be feared. But you do have to be prepared. As pioneers in cyber risk management for over two decades, we understand better than anyone the cyber challenges your clients face. We are the only insurer that offers in house, end-to-end support from quote to breach and back again thanks to our wholly owned cyber security company – Beazley Security. Together with Beazley Security, our Full Spectrum Cyber solution keeps your clients ahead in the battle against cyber risks by pre-empting emerging cyber threats, responding to them, and adapting to new risks as they emerge. It's this constantly moving, evolving approach that makes Full Spectrum Cyber so different from static cyber protection.

Understanding cyber exposures is the first step

Given our everyday activities – both personal and business come with cyber exposure it's essential to have a robust cybersecurity plan in place that will secure people, processes and IT.

The plan should include protection for IT infrastructure, including laptops, devices, servers, IT systems, applications, data and IP assets, networks and cybersecurity training for staff. And what's more, it should be constantly reviewed and evolving – the cyber threats don't stand still and neither should your cybersecurity strategy. Remember it's not just about having sophisticated firewalls and the latest anti-virus software – one accidental click on a phishing email or an out of date application can let the cybercriminals in. Being prepared is key.

Find out more about cybersecurity planning

beazley security

Beware: it's not just cyberattacks that cost money

The value of data and information has increased exponentially. Governments are introducing a range of confidentiality and data privacy laws to keep sensitive customer information private. Fines or penalties may apply for non-compliance with these laws. You may also be legally obligated to notify the affected individuals in the country, state or regional pursuant to applicable laws if their personal or confidential information is inadvertently shared, or lost, stolen or taken due to a data or security breach. Further, you may still be responsible for any such notification obligations, even if you outsource data handling to a third party or cloud provider. Large fines or penalties and costly, lengthy legal court proceedings can follow too.

Common cyber risks and how to build resilience

1 Phishing attacks

Phishing remains one of the most prevalent and damaging cyber threats. Cybercriminals use deceptive emails and websites to trick employees into clicking on malicious links, and divulging sensitive information such as login credentials, financial details, or personal data. The impact can be severe, leading to data breaches, financial losses, ransomware and malware installation and compromised sensitive data.

Beazley Security top tip: Employee training and robust email filtering systems are critical to mitigating this threat.

2 Ransomware

Ransomware attacks have skyrocketed in recent years, targeting businesses of all sizes. In these attacks, malware encrypts a company's data, and the attackers demand a ransom for the decryption key which would allow the targeted company to re-access their systems. Data exfiltration is also increasing, with cyber criminals stealing the data and then demanding a ransom payment for its return. Companies with limited cybersecurity measures are particularly vulnerable. The costs associated with ransom payments, data recovery, and downtime can be devastating.

Beazley Security top tip: A robust, layered approach with 'defence in depth' security is needed to ensure cybercriminals aren't able to access everything, once they are in. Regular data backups and comprehensive endpoint protection are also essential defences against ransomware. Of course avoiding an attack should be the aim so regular phishing assessments, port scans and vulnerability testing are key.

3 Insider threats

Insider threats, whether malicious or accidental, pose a significant risk. Employees, contractors, or business partners with access to sensitive information can inadvertently or intentionally cause data breaches. For businesses without extensive monitoring and access controls, detecting and preventing insider threats can be challenging.

Beazley Security top tip: Implementing strict access controls, continuous monitoring, and employee education can help mitigate this risk.

4 Malware and viruses

Malware and viruses can infiltrate business systems through various vectors, including email attachments, visiting malicious websites, and opening or downloading compromised software. These malicious programs can steal data, disrupt operations, and provide backdoor access to cybercriminals.

Beazley Security top tip: Ensure antivirus and anti-malware solutions are up-to-date and employ advanced threat detection techniques such as Monitoring, Detection & Response platforms (MDR).

5 Weak passwords and authentication

Weak or reused passwords are a common vulnerability that cybercriminals exploit to gain unauthorized access to systems and data. Some businesses struggle with implementing and enforcing strong password policies.

Beazley Security top tip: Utilizing multi-factor authentication (MFA) and educating employees about password security can significantly enhance protection against unauthorized access.

Common cyber risks and how to build resilience

6 Social engineering

Social engineering attacks manipulate individuals into performing actions or divulging confidential information. These attacks can take many forms, including deep fake voice notes and videos, pretexting, (Creating fake identity or scenario to trick a victim into giving confidential information or access to restricted systems) or baiting (fake free offers and downloads that contain malware or request personal details). Companies with less rigorous security awareness training are prime targets.

Beazley Security top tip: Regular training sessions and simulated social engineering attacks can help employees recognize and resist these tactics.

7 Outdated software and systems

Running outdated software and systems exposes businesses to known vulnerabilities that cybercriminals can exploit. Delayed updates and improvements due to budget constraints or operational disruptions are often leading causes for this risk.

Beazley Security top tip: Establishing a regular update and patch management schedule is crucial for maintaining a secure IT environment and avoiding issues with IT platforms as they approach end of life.

8 Data breaches and information theft

Data breaches can occur through various means, including hacking, insider threats, and physical theft. The consequences can include legal penalties, loss of customer trust, and significant financial losses.

Beazley Security top tip: Implementing encryption, access controls, and regular security audits can help protect sensitive data from unauthorized access and theft.

9 Misconfigured cloud resources

Moving to the cloud does not mean moving away from security duties: responsibility for security of cloud resources is most often shared between the customer and the provider. Using default settings, or not paying attention to configuration, can result in data storage or other resources being accessible to unauthorised users.

Beazley Security top tip: Check on the default requirements and ensure updates are carried out. Log and monitor activity, this makes it easier to detect compromises early, and to investigate what occurred. Make sure you read the agreements with your 3rd party providers and understand how their security, monitoring and liabilities are managed.

Responding to a cyber incident

A ransomware message appears when you open your laptop on Tuesday morning. You're locked out and the message says data has been stolen. Questions run through your mind... What's your next move?

"

How did this happen?

What information do they have?

Who can I call?

What do I do now?

How much is this going to cost?

"

In this moment, do you have the know-how to respond?

You'll need help to stop the attack, fix the problem, identify the what's lost, stolen, missing or compromised, manage and resolve compromised systems, and then design and implement a plan to prevent follow-up attacks. Is this level of detail in your Business Continuity Plan and Incident Response Plan? Is your IT team ready to respond or do you have back-up in-place, ready to support you in an instant?

A strong cyber support team can carry you through: a specialist cyber insurance policy not only provides financial protection to cover costs, but also gives you direct access to a range of cyber expertise that helps you respond to a suspected incident at every stage and helps get you back up and running again.

Incident response

- Incident response services
- Investigation and forensics

Specialist expertise to fix the problems

- Data recovery
- Business interruption
- Notification costs
- Legal advice
- Public Relations guidance

Reducing long term impact

- Ongoing legal costs
- Legal & regulatory fines
- Long term security improvements
- Reputation damage

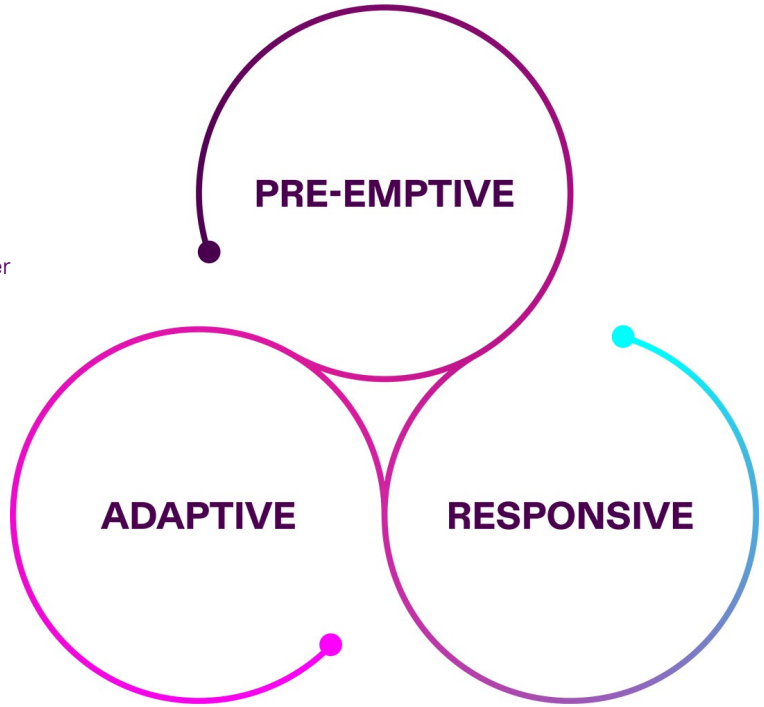
Better protect your business by combining cybersecurity with cyber insurance

In the world of cyber threats, rules don't apply. You need a skilled, fearless, ready-for-anything team at your side.

Protection against the full spectrum of cyber risks

Through our experience of managing thousands of cyber incidents, we know that organisations with integrated cyber risk management services in place develop stronger resilience and are better able to pre-empt, respond and adapt to cyber threats.

By combining our specialist cyber insurance coverages and award winning claims service with Beazley Security's pre & post incident response services, Full Spectrum Cyber focuses as much on keeping our clients one step ahead of the cyber risks as it does getting them back into business quickly should the worst happen.



Pre-emptive Cyber

Stay ready for anything

- Threat intelligence data
- Vulnerability and action plans
- Anti-phishing campaigns and training
- M365 security assessments
- Phishing-resistant MFA keys
- Incident response, business continuity and cybersecurity training for staff and c-suite

Adaptive Cyber

Manage risks as they evolve

- Coverage evolution
- Selected vendors with negotiated rates
- Risk management training
- Cyber tends and data analysis

Responsive Cyber

Get back in the game

- Multiply cyber strengths with cybersecurity experts
- Legal and crisis management
- Forensics and data recovery
- Ransomware negotiatiors
- Public relations consulting and reputational repair
- Claims expertise
- Towers of coverage

Cyber claims in action

Built in cyber incident response services available in an instant

When you partner with Beazley, you instantly multiply your own cyber strength. Any hint of suspicious activity, then one call is all takes for Beazley Security to immediately investigate. And if an incident happens, we mobilise in an instant with access to IT forensics, legal, PR & crisis communications specialists and more to get you back up and running.

Always On' cybersecurity protection

Full Spectrum cyber starts with pre-emptive risk scanning that pinpoint weaknesses and offers access to the right tools, training and risk management tactics that can help prevent cyber-attacks from occurring.

'Always on' Monitoring Detection & Respond (MDR) platforms, available for a fee to complement Full Spectrum Cyber insurance protection, helps to identify and respond to threats and weaknesses before they turn into a full scale incident.

Beazley Security team is constantly scanning the threat landscape. Our clients can expect real time alerts to suspicious activity with instructions and solutions on fixing them, as and when they happen, multiplying your cyber defences.

"We had a client facing foreclosure due to business interruption of £1.2m; their business would have gone into administration which would have led to a significant impact on their credit reputation. We were able to provide an interim claim payment for insured losses to pay the bills, prevent them from folding and preserve their reputation until the claim was fully resolved.

"Employees of a large communications firm were targeted by a phishing campaign. Text messages sent to their personal phones contained a link to a malicious site appearing to be the employer's but designed to harvest username, password, and second-factor code.

Immediately after their incident response team was notified of the campaign, their security operations center opened an investigation, which revealed that 15 employees had entered their credentials into the malicious website. Using the compromised credentials, the hacker accessed internal tools and reset customer email passwords on 27 customer email accounts.

All employees that were compromised had their credentials locked and rotated and the 27 impacted customers had their passwords reset to prevent anyone from accessing the accounts further.

Ready to buy checklist – the essentials for a robust cyber insurance policy

Having a robust cyber insurance policy has become a necessity rather than a luxury. You may be investing in cybersecurity measures already, but no system is ever foolproof. Cyber insurance enables companies to transfer some of the financial risks associated with cyber threats to the insurer.

But how do you know what your business needs?

Here's a checklist to help you evaluate your cyber risks:

Assess your risk profile

- **Data sensitivity:** Consider the type and volume of data your business stores. Personal identifiable information (PII), payment details, and proprietary information are high-value targets for cybercriminals.
- **Regulatory requirements:** Understand the data security compliance requirements specific to your industry, such as GDPR, HIPAA, or PCI-DSS. These regulations often require specific levels of protection and reporting, which should be reflected in your insurance coverage.
- **Contractual obligations:** Some contracts, especially with larger companies or government entities, may require you to carry a specific amount of cyber insurance.

Understand the potential financial impact of a cyber attack

- **Cost of data breach:** Consider the cost of a potential data breach, including computer forensics, data recovery, notification costs, legal fees, regulatory fines, and public relations efforts.

  Business interruption: Factor in the potential loss of income if your operations are disrupted by a cyber event.
- **Ransom payments:** If your business could be a target for ransomware, consider the potential ransom demands.
- **Reputational damage:** Consider the potential long-term impact on your reputation and customer trust, which might require additional marketing or communication efforts to repair.

Additional expert cyber support

- Do you need access to cyber experts when an issue happens? Consider what help you need, forensic experts, legal advisors, and public relations firms, all which can be crucial during a crisis.

Identify the scope of coverage

Coverage varies and so does the type and level of protection.

- A good insurance broker can assess your specific needs, exposures and potential financial impacts to recommend appropriate coverage and tailor the policy to cover:

  First-party coverage: This includes financial costs directly associated with a cyber incident, breach or system failure, such as data recovery costs, business interruption losses, and cyber extortion negotiations and payments associated with a ransomware attack.
- **Third-party coverage:** Protects against claims made by customers, partners, or other third parties affected by a cyber incident at your business. This includes lawsuits, regulatory defence and penalties, legal fees, settlements, and regulatory fines.
- **Incident response costs:** Ensure your policy covers the cost of hiring experts for forensic investigations, public relations, and legal consultation following a breach.
- eCrime provides first party protections against loss of funds due to fraudulent instruction or funds transfer fraud.

Discover more
beazley.com

About the authors

Beazley is a global specialist insurer and a pioneer in cyber insurance for over two decades. Together with Beazley Security, its wholly-owned cybersecurity firm, they share a joint aim to reduce risk and increase cyber resilience for all.

xxx

For more information, please go to: beazley.com

beazley

beazley security