WHITEPAPER

HOW CYBER INSURANCE HAS CHANGED IN 2021/2022

P2 Technologies
a PAV IT company

Ppavilion

A few years ago, cyber insurance could be purchased with minimal form filling and a basic understanding of IT security. Cybercrime has relentlessly increased in business and the effect on IT, recovery time and cost as well as frequency of attacks. Rising ransomware attacks are the key reason our customers seek cyber insurance.

Businesses are choosing cyber insurance either having directly suffered from a cyber-attack, sector specific and focused attacks or to balance weaknesses in IT security. Together with increasing flexibility of IT being accessed from anywhere, insurance companies are requiring a far more detailed assessment to the security controls in place prior to the provision of cyber insurance policies. In doing so, they are balancing their own risks and mitigating the chances of having to pay out during or after a cyber incident.

When completing cyber insurance forms, the amount of information required can appear daunting. Larger businesses generally have the resources and technology in place to manage their own IT security and flex as new threats emerge. Smaller businesses seek the same level of protection and it's knowing where to start without being overwhelmed.

Cyber insurance providers have recently suffered heavy losses, and this has had a material effect to the number of active providers who are prepared to take on cyber risk. Fewer cyber insurers means less supply and with that a positive effect on premiums which have inevitably increased for the same level of coverage. At the same time, it is a supplier's market, and they are becoming more selective as to who they will insure and what information they require. Incremental time and effort fall upon the customer simply to provide sufficient information to qualify for a cyber insurance policy.

We've combined the most common security controls that are asked for in cyber insurance proposal forms in 2022 to help focus your priorities, aiding the completion of proposal forms, improving your security position, saving time, and helping you to place a cap on rising insurance premiums.

Information security standards

All businesses should aim to attain an industry standard towards data security. These standards are frameworks which are key in so far as they provide outlines of what is to be considered a minimum attainable standard for IT security as well as the protection of business and customer data. These standards also outline a requirement on the processes that organisations must build into their systems that cover a multitude of weaknesses. The benefit of cyber insurance together with working towards a security standard is driving continual improvement in cyber security. If a cyber-attack or ransomware is experienced, then it often takes weeks to recover. A focus on standardisation and testing is of upmost importance.

We are seeing 4 common information security standards being asked for on cyber insurance proposal forms, Cyber Essentials, Cyber Essentials Plus, IASME and ISO 27001.

Many businesses aim to have one or multiple of these standards. Depending on their attitude to IT security risk, the confidentiality or value of their business or customer data and what the supply chain implications are if you are affected.

Achieving any of these standards will aid the completion of the cyber proposal forms as many of the controls are covered in these standards.

Cyber Essentials and Cyber Essentials Plus (the latter being more comprehensive and audited) is a good starting standard, mainly questionnaire based and relatively inexpensive for all businesses to achieve and shows suppliers and customers that you're focused on IT security.

ISASME (Information Assurance for Small and Medium Enterprises) Government backed goes further than Cyber Essentials by focusing on your risk and an assessment against GDPR.

ISO 27001 is an internationally recognised standard focused on information risk management, providing policies, processes and standards and controls to protect data. ISO 27001 is rigorous and audited.

Attaining one or more of these standards has a secondary effect in so far as it boosts your own customer confidence that they are in business with an organisation fully invested in IT and takes IT security seriously.

Access & Security Controls

Backup: to minimise ransom payments and recover faster there is more emphasis on the importance of disaster recovery planning and preparation. Most cyber incidents will resort to recovery of file or server systems. Backup and recovery is the ultimate back stop to getting the business back up and running.

Review your backups, where is the data located (both on and off site), how often and what data? What is the retention period for the backup files and have you a documented procedure for backup and recovery of data and services to get the business up and running?

Password management: apply multi-factor authentication (password and separate token) on every computer, appliance, and application. If passwords are breached it is much more difficult for perpetrators to access your systems.

Antivirus: does your antivirus include anti-ransomware technology? Does it have machine learning capability to spot zero-day threats? Can your antivirus system be managed to contain sideways movement of cyber threats on your network or further still have a managed threat protection and reporting system?

Operating and application patching: no software or operating system is perfectly secure and cyber criminals expend huge effort to find issues known as exploits that invariably allow access. Almost on a weekly basis, software vendors make available security or functionality updates and these need to be applied as soon as is practical to do so. You should consider how you apply patches to applications and devices, how often they are applied, whether you have a reporting capability and most importantly, what can be automated to help administer updates and thereby manage the threat of unpatched systems or applications.

System age: are the operating system and applications you use still supported and security updates being made available by your vendors? If not, can these systems be upgraded, can they be switched off or should they be moved to secure networks with no internet facing IP address to mitigate your risk?

Data encryption: Is data on your systems encrypted locally and in transit (mobile device or devices connected in remotely)? The encryption can apply to file, databases, and mobile devices.

People: are often overlooked but we can assure you that your employees are often the weakest link with respect to targeted phishing or ransomware attacks. So, ask yourself some questions:

- Do you know who has access to your systems and to what – this can be internal staff to external suppliers?
- Do you have procedures for adding and removing staff and third parties from your systems?
- Do you regularly train your staff on managing security from simulated phishing to questionnaires on computer use?

Policies: it is vital that you document critical processes for reference. The items we would ask our clients to prioritise are:

- Do you have a policy on how old data is managed and retained?
- Do you have a business continuity and disaster recovery plan and is it tested? (Business continuity – plan and systems to keep critical business systems operational, disaster recovery the ability to recover).
- Do you have a privacy policy that describes the way in what data is managed by systems?
- Information security policy written and communicated to staff – having the best technology available is useful, however only if staff know what is required of them using your systems.

Cyber crime controls: have you applied check and balances that will hinder staff from independently choosing to pay or carry out specific acts without consultation, such as paying larger invoices? The following will help to mitigate against unauthorised / unchecked transactions:

- Do you have a payment authorisation and bank details check process to validate authenticity?
- Do you have a process to authorise payment over a certain value?
- Do you have a process or technology to cap or notify excess premium rate numbers? – some modern phone systems can do this automatically.

Summary

Cyber insurance and its requirements are going to continue to change as IT and cybercrime continues to evolve. Cyber insurance premiums are likely to continue rising with policies becoming ever scarcer as the providers alleviate both the rising complexity, increase in claims and fewer policies available to purchase. At this time, risks and prices are on a relentless upward trajectory and a focused effort is now required to reduce your risk profile and in doing so, to improve your insurability weighting with cyber insurance providers. This will mean the greatest choice of products and the best insurance terms.

Building security standards into your business planning will improve your security posture. Many of the controls required within the standards will have a positive impact on your risk profile and therefore your insurability and premiums.

If following the review of this white paper, you have additional questions or need more support then please rest assured in the knowledge that we regularly help our clients review cyber insurance proposal forms. We can help you to understand the requirements of the industry standards and we are able to help you implement appropriate technologies that policies and standards require.

To learn more about how PAVilion can help support your organisation, please contact info@pav.co.uk

The Old Corn Mill, Bullhouse Mill
Lee Lane, Millhouse Green
Sheffield S36 9NN

Tel: 01273 834 000
Email: info@pav.co.uk
URL: www.pav.co.uk

P2 Technologies a PAV IT company

pavilion