DigitalXRAID
CYBER SECURITY EXPERTS

CYBER INSURANCE

How ISO 27001 Can Reduce Cyber Insurance Premiums

Cyber insurance has become a necessity to protect businesses from cyber threats

As businesses increasingly rely on technology and digital systems, the need for cybersecurity measures becomes more critical than ever. Cyber threats can cause significant financial losses, reputational damage, and legal consequences.

Cyber insurance has become a necessity to protect businesses from cyber threats. However, cyber insurance premiums are becoming increasingly expensive and restrictive, and businesses need to find ways to reduce their costs.

ISO 27001 is a globally recognised standard that defines best practices for information security management systems (ISMS). By implementing ISO 27001, companies can demonstrate that they have a well documented and monitored system in place to manage and protect their information assets.

This includes identifying and assessing risks, implementing controls to mitigate risks, and regularly reviewing and improving the ISMS.

By obtaining ISO 27001 certification, businesses can demonstrate to insurers that they are taking a proactive approach to cybersecurity with robust cybersecurity measures in place.

This can lead to reduced cyber insurance premiums, as insurers see ISO 27001 certification as evidence that the business has implemented appropriate security measures, making them less of a risk.

In addition to reduced premiums, businesses that obtain ISO 27001 certification can also benefit from improved risk management, increased customer confidence, and enhanced business resilience.

In this ebook, we'll discuss in more detail how obtaining ISO 27001 certification can help businesses save money on cyber insurance premiums.

Understanding Cyber Insurance

Cyber insurance is based on the concept of risk transference. In return for the premiums paid, the insurer agrees to cover the financial losses incurred by the policyholder in the event of a cyber incident.

Cyber insurance policies can cover the financial losses that result from cyber incidents such as data breaches, malware attacks, and network downtime. Cyber insurance policies typically also cover expenses related to crisis management, investigation, legal fees, and reputational damage.

The coverage can extend to loss of income and expenses related to business interruption caused by cyber incidents, depending on the policy taken.

However, cyber insurance policies are becoming more restrictive and expensive due to the rise in cyber threats.

The cost of cyber insurance policies varies depending on the level of risk and coverage required. Insurers evaluate a business's cybersecurity posture and assign a risk level based on factors such as the type of data held, where that data is stored, the security controls in place, and the size of the business.

Cyber insurance premiums can range from a few hundred pounds to hundreds of thousands of pounds per year.

Insurers are now taking a more cautious approach to cyber insurance, due to the constantly evolving nature of cyber threats. The increased frequency and sophistication of cyberattacks has led insurers to increase premiums and restrict coverage.

Insurers are also cautious of offering coverage for nation-state attacks as the scale and complexity of these attacks are beyond the scope of many businesses and insurance policies.

ISO 27001 certification can help businesses reduce their cyber insurance premiums by demonstrating to insurers that they have implemented effective cybersecurity measures.

Insurers are more likely to offer lower premiums to businesses that can demonstrate a good cybersecurity posture and a proactive approach to managing cyber risks.

ISO 27001 certification provides a framework for implementing effective information security management systems, which can help businesses identify and mitigate cyber risks.

By obtaining ISO 27001 certification, businesses can reduce their cyber risk profile and demonstrate their commitment to cybersecurity to insurers.

Insurers are more likely to offer lower premiums to businesses that can demonstrate a good cybersecurity posture and a proactive approach to managing cyber risks.

Cyber Threats

Cyber threats are diverse and ever evolving, making it challenging for businesses to stay ahead of them.

Cybercrime is a growing problem, and hackers continue to develop sophisticated attack methods.

According to a report by Hiscox, nine out of ten companies experienced at least one cyber incident in the last 12 months. With such a high likelihood of experiencing a cyber incident, businesses must take proactive measures to protect their systems and data.

Ransomware is a type of malware that encrypts a victim's files, rendering them inaccessible until a ransom is paid. Ransomware attacks have become a significant concern for businesses, with an increase in attacks reported over the past year.

According to an industry report, ransomware attacks increased by 151% over just 6 months, with one month seeing a 38% increase alone. The report also revealed that the average ransom payment had increased by 82% during the same period.

The impact of a cyberattack can be significant, causing disruption to business operations, reputational damage, and financial losses.

Ransomware attacks can be particularly devastating, as they involve encrypting a business's data and demanding a ransom payment in exchange for the decryption key.

However, paying the ransom is not recommended, as it can encourage attackers to continue their activities and may not guarantee the return of the data.

In addition to ransomware attacks, other types of cyber threats, such as phishing attacks, social engineering, and malware attacks, remain a significant concern for businesses.

Cybercriminals are constantly developing new techniques to exploit vulnerabilities and gain unauthorised access to systems and data.

In recent years, there has been a significant increase in the threat of nation-state attacks, particularly.

These attacks are often highly sophisticated and coordinated, targeting critical infrastructure and high-value targets.

> **“ Insurers have responded by increasing premiums for cyber insurance policies**

Some insurers, such as Lloyds of London, have stated that they will no longer offer cover for nation state attacks due to the substantial risk and complexity involved.

Cyber Insurance Costs

Cyber insurance premiums vary depending on the level of risk and coverage required. The cost is also affected by the number of claims made by businesses in the same industry.

As cyber insurance is still a relatively new class of insurance, premiums can be high, and businesses need to be cautious about obtaining policies that overlap with other insurance policies.

It is essential to carefully review the coverage provided by a policy and seek advice from an insurance broker.

In recent years, the frequency and severity of cyber incidents have increased significantly, leading to a surge in demand for cyber insurance coverage.

With businesses of all sizes facing the risk of cyberattacks, cyber insurance has become a necessary protection mechanism. However, the cost of cyber insurance premiums has been increasing, making it challenging for businesses to afford adequate coverage.

According to a report by Coalition, a US-based cyber insurance provider, the average cost of a cyber insurance policy in the US increased by 22% over just 12 months.

The same report showed that the frequency of ransomware attacks increased by 486%, and the average ransom demand increased by 47% compared to the previous year. This highlights the growing severity and cost of cyber incidents.

In the UK, a report by Hiscox revealed that the average cost of a cyber incident for businesses was £2.9 million, with the most significant losses being attributed to reputational damage and business interruption.

The report also highlighted that small businesses were particularly vulnerable, with 47% of surveyed small businesses experiencing a cyber incident within the last 12 months.

The recent increase in cyberattacks and severity of incidents has prompted cyber insurers to adopt stricter underwriting practices and increase premiums.

Insurance companies are starting to focus more on risk management and loss prevention, which means businesses must demonstrate that they have robust cybersecurity measures in place.

Insurers are now conducting more thorough assessments of a business's cybersecurity posture before providing coverage. This includes reviewing a business's policies, procedures, and controls relating to data protection, network security, and incident response.

Any gaps in a business's cybersecurity posture could lead to higher premiums or even a rejection of coverage.

Another factor driving up cyber insurance premiums is the rise in ransomware attacks.

Cybercriminals are increasingly using ransomware to extort money from businesses by encrypting their data and demanding payment in exchange for the decryption key.

Insurers are now taking a more cautious approach to providing ransomware coverage, which has led to higher premiums.

It is essential to note that paying a ransom demand to a cybercriminal only exacerbates the problem. Not only does it fund criminal activity, but it also does not guarantee the return of data or systems.

The best approach is to have adequate cybersecurity measures in place to prevent ransomware attacks and to have a robust incident response plan in case of an attack.

Businesses looking to reduce their cyber insurance premiums should consider implementing ISO 27001 as a proven method for reducing cyber risk.

Obtaining ISO 27001 certification demonstrates that a business has a robust information security system in place, reducing the likelihood of a cyber incident.

> **Ransomware attacks account for 41% of all cyber insurance claims**

ISO 27001 and Cybersecurity to Reduce Premiums

ISO 27001 is a widely recognised international standard that outlines the best practices for information security management. The standard provides a framework for implementing an information security management system (ISMS) to protect the confidentiality, integrity, and availability of information.

The ISMS covers all aspects of information security, including physical, technical, and legal aspects.

ISO 27001 certification is achieved by implementing and maintaining an ISMS that meets the requirements of the ISO 27001 standard. The standard requires businesses to conduct a risk assessment to identify potential threats and vulnerabilities to their information assets.

Based on that risk assessment, businesses must develop a risk treatment plan that includes controls to mitigate identified risks. The standard also requires businesses to have a continual improvement process in place to ensure that the ISMS remains effective over time.

By implementing ISO 27001, businesses can address the vulnerabilities in their information security systems, reducing the likelihood of a cyber attack occurring. This can lead to improved business resilience and customer confidence.

The implementation of an ISMS based on ISO 27001 can bring several benefits to businesses beyond reducing cyber insurance costs. Certification can enhance the reputation of a business as a trusted and secure organisation, which can be a competitive advantage.

The implementation of an ISMS involves several stages, including the development of policies and procedures, implementation of security controls, staff training, and ongoing monitoring and review.

Once the ISMS has been implemented, an external auditor will assess the system's effectiveness and compliance with the ISO 27001 standard.

ISO 27001 certification is a rigorous process that requires a significant investment of time and resources. By outsourcing ISO 27001 certification to a security services provider, gap analysis, implementation, audits and ongoing management and certification maintenance are all fully managed.

Some insurers offer discounts on cyber insurance policies for businesses that have achieved ISO 27001 certification. According to a study by UK-based insurance company CFC Underwriting, businesses with ISO 27001 certification are 22% less likely to experience a data breach than non-certified businesses.

The study also found that certified businesses that experienced a data breach had lower overall losses than non-certified businesses that suffered similar breaches.

It is important to note that achieving ISO 27001 certification does not guarantee that a business will not experience a cyber incident or reduce the likelihood of a cyber incident occurring.

However, the implementation of an ISMS based on the standard can help businesses minimise the risk of cyber incidents and demonstrate to insurers that they have taken proactive measures to reduce the risk of cyber incidents.

In addition to potentially reducing cyber insurance costs, implementing an ISMS can help businesses improve their overall security posture, reduce the likelihood and impact of cyber incidents, and meet legal and regulatory requirements.

Furthermore, the certification can enhance the reputation of a business as a trusted and secure organisation, which can be a competitive advantage in today's digital economy.

The benefits of certification can be significant for businesses.

Those that prioritise information security and seek to demonstrate their commitment to protecting their systems and data from cyber threats will reap the benefits of reduced cyber insurance premiums.

Understanding Cyber Insurance

Obtaining ISO 27001 certification can help businesses mitigate cyber risks in several ways.

1

Firstly, ISO 27001 requires businesses to maintain specific documentation on their IT assets and process flows, both internal and external.

This documentation provides transparency into how information is handled, allowing businesses to identify potential vulnerabilities and develop strategies to address them.

By having a well-documented and monitored system in place, businesses can be confident that they are adequately prepared to face an insurer and save money when concluding cyber insurance contracts.

2

Secondly, ISO 27001 certification requires businesses to conduct regular risk assessments to identify potential security threats and vulnerabilities.

The risk assessment process involves identifying assets and information that need protection, analysing potential threats, and assessing the likelihood and impact of a security breach.

This process allows businesses to prioritise their security measures and allocate resources effectively.

3

Finally, ISO 27001 certification requires businesses to implement a management system to monitor and maintain the effectiveness of their security controls.

By showing that they have taken proactive measures to protect their data and systems, companies can enhance their reputation and build trust with their stakeholders.

Certification helps businesses to demonstrate their commitment to cybersecurity to customers, partners, and other stakeholders

By staying up to date with the latest cybersecurity best practices and standards, businesses can stay ahead of potential cyber risks and reduce their exposure to cyberattacks.

Cyber insurance policies are becoming more restrictive and expensive. Companies need to take a proactive approach to cybersecurity to protect against online threats.

Proactive cybersecurity measures are essential and beneficial for businesses to reduce their cyber insurance premiums and prevent cyberattacks.

One of the best places to start this journey is with ISO 27001 certification.

By obtaining ISO 27001 certification, businesses can demonstrate their commitment to cybersecurity to customers, partners, company stakeholders, insurers, enhance their reputation, and build trust.

> **“Companies need to take a proactive approach to cybersecurity to protect against online threats**

How can we help?

By utilising our ISO 27001 certification and Cyber Maturity Assessment services, DigitalXRAID has extensive experience in working with organisations to reduce the cost of their cyber insurance premiums.

DigitalXRAID will provide you with a fully managed ISO 27001 service, taking you step-by-step through the entire process through to certification.

This includes an initial gap analysis and implementation, right up to the certification stage 2 audit.

Not only that – once you've achieved your certification our highly trained experts will continue to provide support and advice, safeguarding your business and ensuring you remain compliant and exceed ISO 27001 requirements.

The DigitalXRAID team have never had a customer fail an audit or receive a major non-conformance.

By partnering with DigitalXRAID, businesses can confidently take proactive measures in protecting their systems and data against cyber threats, achieve ISO 27001 certification, decrease risk, and effectively reduce cyber insurance premiums.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 27001 INFORMATION SECURITY MANAGEMENT

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 8289 ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

CREST

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing