Cyber Risk and Small and Medium-Sized Businesses

Making robust cybersecurity measures more critical than ever.

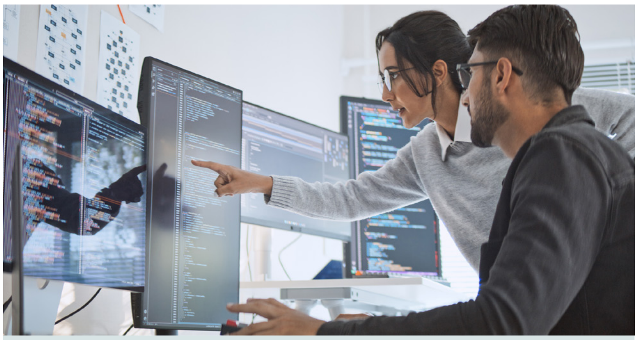
Contents

Cyber Risk and Small and Medium-Sized Businesses

In today's digital landscape, small and medium-sized businesses (SMBs) are increasingly vulnerable to cyber threats, making robust cybersecurity measures more critical than ever. A cyber emergency—defined as any incident that compromises the integrity, confidentiality or availability of an organisation's data—can strike at any moment, leading to significant operational disruptions, financial losses, and reputational damage.

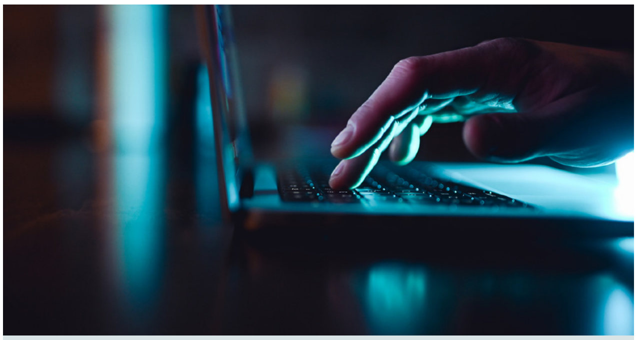
SMBs are not immune to the threat of cybercrime:

- **46%** of all cyber breaches impact businesses with fewer than 1,000 employees according to Verizon's 2021 Data Breach Investigations Report.[1]
- **One** in three small and medium-sized businesses have experienced a cyber-attack.[2]
- **81%** of SMBs say AI increases the need for additional security.[3]
- **Less** than one in five SMBs have a cyber insurance policy.[4]



The role of legislation in shaping cybersecurity practices cannot be overstated.

Compliance with regulations such as the Consumer Protection Act (CPA), Electronic Communications and Transactions Act (ECT), the Protection of Personal Information Act (POPI) and various industry-specific standards not only protects businesses from legal repercussions, but also reinforces commitment to safeguarding customer data and trust.



The consequences of a cyber event can be particularly severe for SMBs. Beyond the direct financial impact—often estimated to reach thousands or even millions of Rand—there are long-term effects, including loss of customer confidence, diminished market share and potential business closure. As cyber threats evolve, it is imperative for SMBs to recognise the urgency of implementing comprehensive cybersecurity strategies that include effective response planning and adherence to relevant legislation, in addition to offsetting the risk with appropriate insurance covers where necessary.

This whitepaper delves into the multifaceted cyber risks faced by SMBs, highlighting the critical importance of preparedness, the formation of dedicated response teams and the imperative of legal compliance in safeguarding business integrity in the face of emerging and constantly evolving cyber threats.

What is a Cyber Emergency

In today's digital landscape, SMBs face an increasing array of cyber threats that can disrupt operations and compromise sensitive information. Data breaches, hacking attacks, and malicious software (malware) attacks represent significant cyber emergencies that can have devastating effects on an SMB's reputation, financial stability and operational integrity.

A data breach can lead to the exposure of customer and employee information, resulting in loss of trust and potential legal repercussions. Hacking attacks may result in unauthorised access to critical business systems, causing downtime and financial loss. Similarly, malware attacks can incapacitate an organisation's IT infrastructure, leading to data loss and operational paralysis. As the cyber threat landscape evolves, the urgency for SMBs to adopt robust cybersecurity measures has never been more critical to safeguard their assets and ensure business continuity.

Cyber emergencies include:

Data Breaches

A data breach occurs when unauthorised individuals gain access to sensitive data, such as personal information, financial records, or business Intellectual Property (IP). This can happen due to weak security measures, insider threats, or cyberattacks. The exposed data can be used for identity theft, fraud or sold on the dark web.

Hacking Attacks

Hacking attacks involve unauthorised access to computer systems or networks with the intent to steal, alter, or destroy data. Hackers may exploit vulnerabilities in software, use social engineering techniques, or deploy various tools to gain access. The motives can range from financial gain to political activism or simply for the challenge.

Malicious Software Attacks

Malware refers to any software specifically designed to harm or exploit devices, networks, or services. Types of malware include viruses, worms, trojans, ransomware, and spyware. These can lead to data theft, system damage, or unauthorised access to sensitive information.

Denial of Service (DoS) Attacks

A DoS attack aims to make a system or service unavailable by overwhelming it with traffic or exploiting vulnerabilities. In a distributed denial of service (DDoS) attack, multiple compromised systems are used to flood the target, causing it to crash or become inaccessible to legitimate users.

Cyber Extortion Attacks

Cyber extortion involves threatening to harm a victim's data or systems unless a ransom is paid. This can take the form of ransomware attacks, where attackers encrypt a victim's files and demand payment for the decryption key, or threats to release sensitive information publicly if a ransom is not paid.

The Value of Having a Cyber Emergency Response Team

If an SMB falls victim to a cyberattack, having a robust response plan in place is crucial. A dedicated cyber emergency response team provides invaluable support, offering unlimited 24/7 access to a team of cybersecurity specialists. This team not only delivers proactive guidance on security issues. but also coordinates post-incident services, assists with breach responses and offers expertise in data privacy and crisis management. With their skills in forensic investigation and remediation, these experts ensure that SMBs can effectively navigate the complexities of cyber emergencies, minimising impact and fortifying defences against future attacks.

When a cyber emergency occurs, an SMB will most likely need a cyber emergency response team for these key reasons:

1. **Proactive Guidance:** provide ongoing advice to enhance cybersecurity measures, helping to prevent future incidents.
2. **Post-Incident Coordination:** effectively coordinate response efforts after a cyber incident, ensuring that all necessary actions are taken in a timely manner.
3. **Breach Response and Notification:** assists in managing breach notifications to affected parties and regulatory bodies, ensuring compliance with legal requirements.
4. **Data Privacy Expertise:** navigate the complexities of data privacy laws and best practices, minimising legal risks.
5. **Crisis Management:** strategic support during a crisis, helping to manage communication and public relations.
6. **Forensic Investigation:** conduct thorough investigations to determine the cause and impact of the breach, identifying vulnerabilities for future prevention.
7. **Remediation Support:** implementing effective remediation measures to restore systems and secure data.

Having a dedicated cyber emergency response team available provide the business with the means to tap into the necessary expertise needed to respond swiftly and effectively to cyber threats, minimising damage and downtime.

Cyber Risk and Legislation

A cyber breach has the potential to inflict enormous reputational damage, cause major interruption to normal business operations, as well as current and future income potential, and can also have legal liability ramifications if personal and financial information is compromised.

Consumer Protection Act (CPA)

The CPA promotes a fair and transparent marketplace, protecting consumers' personal information and ensuring ethical marketing. It gives consumers the right to privacy, prohibits misleading digital marketing and provides recourse for unfair or unsafe online transactions.

Electronic Communications and Transactions Act (ECT)

The ECT Act gives legal recognition to electronic contracts and signatures, enabling e-commerce while protecting consumers online. It also defines cybercrime offences such as hacking and data interception, reinforcing accountability in digital transactions.

Protection of Personal Information Act (POPIA)

POPIA safeguards individuals' privacy by requiring consent for data processing, granting rights to access and correct personal data, and holding organisations accountable for maintaining robust security controls to prevent breaches.

Joint Security Standard (JSS)

The Joint Security Standard complements these laws by setting out best-practice guidelines for cybersecurity governance, risk management and incident response. It promotes collaboration between industries to align security controls, strengthen resilience and ensure compliance with legal and regulatory requirements.
By adopting the JSS framework, organisations can better demonstrate due diligence, improve data protection and enhance stakeholder trust.

Together, these frameworks require every organisation - especially SMBs - to maintain effective compliance and security processes. Failure to do so can result in regulatory penalties, reputational damage and significant operational risk.

What Cyber-related Losses Could Your SMB Suffer?

Cyber risk is omnipresent for small to medium-sized businesses (SMBs) and among the threats, three significant types of losses stand out:

- business interruption loss,
- data restoration costs and,
- cyber extortion costs.

Each of these can disrupt operations, drain resources and pose long-term challenges to business viability. Understanding these implications is crucial for SMBs as they navigate the complexities of cybersecurity and strive to protect their assets and reputation.

Business Interruption Loss

Business interruption loss refers to the financial impact that occurs when a business cannot operate due to a cyber incident, such as a ransomware attack or system outage. For an SMB, this can be particularly devastating. The costs may include:

- **Lost Revenue:** If operations are halted, the business loses sales and profits, which can significantly affect cash flow. For instance, if a retail SMB loses a week of sales during peak season, the revenue lost could be substantial.
- **Ongoing Expenses:** Even if the business isn't generating revenue, fixed costs (like rent, utilities, and salaries) continue to accumulate, further straining finances.
- **Reputational Damage:** Prolonged outages can lead to customer dissatisfaction and damage the brand's reputation, potentially resulting in lost future business.

Data Restoration Costs

Data restoration costs arise when an SMB needs to recover lost or corrupted data after a cyber incident. This can include:

- **Backup Solutions:** The business may need to invest in reliable backup and recovery solutions, which can range from cloud services to physical storage, depending on the volume and sensitivity of the data.
- **IT Support and Labor:** Restoring data often requires hiring IT professionals or utilising internal resources, which can be costly, especially if the restoration process is complex or lengthy.
- **Downtime During Restoration:** The time taken to restore data can lead to additional business interruption, compounding the financial impact.

Cyber Extortion Costs

Cyber extortion typically involves a threat to release sensitive data or to render systems inoperable unless a ransom is paid. The implications for an SMB can include:

- **Ransom Payments:** If an SMB opts to pay the ransom (which can vary widely in financial quantum), this creates an immediate financial burden. The decision to pay also raises ethical considerations and does not guarantee that the threat will be resolved.
- **Legal and Compliance Costs:** Depending on the nature of the data involved, the business may have legal obligations to notify affected parties, which can lead to further costs associated with legal fees, regulatory fines, or lawsuits.
- **Increased Cybersecurity Measures:** After an extortion incident, businesses often need to invest significantly in cybersecurity to prevent future incidents, which can include hiring experts, purchasing software, and training staff.

These cyber-related losses and increased cost of doing business can have profound and lasting effects on SMBs, impacting their financial stability, operational efficiency and overall business continuity. The necessity of proactive cybersecurity measures has never been more critical for protecting against these risks.

As SMBs deepen their digital presence, they also expose themselves to potential liability for third-party claims related to cybersecurity incidents. This includes a range of financial risks, such as liability for data breaches affecting clients or partners, multimedia liability claims arising from content published online and regulatory expenses linked to non-compliance with data protection laws. Additionally, businesses may face PCI (Payment Card Industry) fines and penalties if they fail to adequately secure payment information. These liabilities can further compound the financial impact of cyber incidents, highlighting the importance of robust cybersecurity measures and legal compliance for protecting both the business and its stakeholders.

In addition, there are also likely to be emergency response costs pertaining to:

- Forensic costs
- External legal fees
- Notification costs for data breaches
- Call centre for queries related to data breaches
- Credit monitoring

By analysing exposures, taking steps to address risk and establishing a strategy for assembling a claim quickly and accurately, businesses can better prepare themselves for the threat of a cyber incident.

How Can I Protect My SMB From a Cyber Event?

Implementing robust cybersecurity measures such as antivirus software, email security, vulnerability reporting and regular backups is essential for small and medium-sized businesses (SMBs) to defend against cyber threats.

Antivirus programs provide real-time protection against malware and other malicious software, while email security safeguards against phishing attacks and spam that could compromise sensitive information. Vulnerability reporting helps identify and address potential weaknesses in the system before they can be exploited by attackers.

Additionally, regular backups ensure that critical data can be restored quickly in the event of a breach or ransomware attack, minimising downtime and financial loss. Together, these measures create a comprehensive defence strategy, enabling SMBs to operate securely and with confidence in an increasingly digital landscape.

AntiVirus

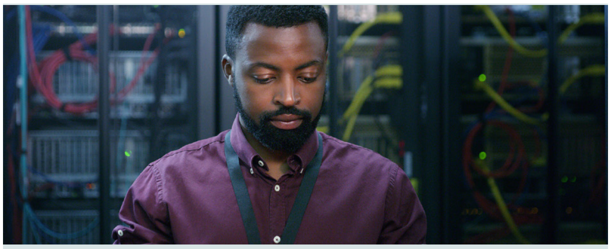
Complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. Its prevention-first approach ensures your organisation is not exposed to attacks and it simplifies your security operations.

E-mail Security

Provides complete protection for Microsoft 365, Google Workspace and all your collaboration and file-sharing apps. It is the ONLY solution that prevents, not just detects or responds to, threats from entering the inbox.

Vulnerability Reporting

This assesses the security structure of an organisation from an attacker's perspective. The method strives to close off all the entry points of intrusive attacks, and weaknesses from the network's firewall. These external vulnerability scans help prioritise remediation efforts and reduce the attack surface of a company's external network.



Back-up

To overcome the growing complexity of IT infrastructures and sophisticated cyberattacks requires a comprehensive backup solution to keep data safe. Backup individual files or your entire business by backing up entire systems as a single file. In the event of data disaster, you can restore all information from back-up to new hardware.

How Aon can help

Aon conducted a cyber risk survey in South Africa, and it was clear from the survey findings that SMBs simply do not have the resources to effectively deal with a cyber event.

In solving this challenge, Aon's bespoke, consolidated cyber risk solution for SMBs brings together and leverages both the cyber security solutions required, and the insurance carrier requirements to provide a competitively priced proposition.

For SMBs that opt for this cyber bundle, a specialist insurer will pre-qualify clients for cyber insurance coverage that provides SMBs with all the key services and support required when dealing with a cyber event. This solution is key to alleviating many of the resource constraints experienced by SMBs, driven largely by the increase in regulation and compliance requirements facing SMBs in their operations.

For more information and to get a quote, click Here.

The below table outlines the basis of the solution:

Phishield Basic Cyber Cover	CyberSafe's Basic Cyber Controls
Cyber Extortion Threat & Cost Costs to investigate and resolve Cyber Extortion. Threats including ransom payments	**Anti-Virus** Complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. Its prevention-first approach ensures your organization is not exposed to attacks and it simplifies your security operations.
Data Restoration Costs Costs to regain, replace or restore data that is damaged, lost or corrupted due to a Cyber Incident.	**E-Mail Security** Provides complete protection for Microsoft 365, Google Workspace and all your collaboration and file-sharing apps. It is the ONLY solution that prevents, not just detects or responds to, threats from entering the inbox.
Third Party Claims A written notice of demand/pending legal action/ regulatory action seeking compensation/regulatory penalties/legal remedies	**Vulnerability Reporting** This assesses the security structure of an organization from an attacker's perspective. The method strives to close off all the entry points of intrusive attacks, and weaknesses from network's firewall. These external vulnerability scans help prioritise remediation efforts and reduce the attack surface of a company's external network.
Multimedia Liability Claims Damages and defence costs for Your Business is legally obligated to pay for defamation, infringement of IP, data extraction, non-conformance to legal requirements relating to discrimination on website, social media, etc.	**Back-Up's** Backup individual files or your entire business by backing up entire systems as a single file. In the event of data disaster, you can easily restore all information to new hardware.
Business Interruption Loss Operating profits, which cannot be earned during the total or partial interruption to the Computer System, plus fixed operating expenses as a result of a Cyber Emergency.	
Regulatory Expenses and Penalties Fines/penalty by government /regulator following regulatory investigation. Contractual fines and penalties due to breach of PCI Security Standards.	

References:

1. Verizon's 2021 Data Breach Investigations Report.
   Located at: https://www.verizon.com/business/resources/reports/dbir/2021/smb-data-breaches-deep-dive/

2. Microsoft Industry Trends Report: 7 cybersecurity trends and tips for small and medium businesses to stay protected.
   Located at: https://www.microsoft.com/en-us/security/blog/2024/10/31/7-cybersecurity-trends-and-tips-for-small-and-medium-businesses-to-stay-protected/

3. Microsoft Security: Small and medium business (SMB) cyberattacks are frequent and costly.
   Located at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/SMBCybersecurity-Report-Final.pdf

4. Aviva: One in five businesses have been victims of cyber attack in the last year.
   Located at: https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/

Disclaimer

The information contained herein and the statements expressed should not be considered or construed as insurance broking advice and are of a general nature. The information is not intended to address the circumstances of any particular individual or entity. Accordingly, the information contained herein is provided with the understanding that Aon, its employees and related entities are not rendering insurance broking advice. As such, this should not be used as a substitute for consultation with an Aon Broker or Consultant.

Although we endeavour to provide accurate and current information and we use sources we consider reliable, Aon does not warrant, represent or guarantee the accuracy, adequacy, completeness or fitness for any purpose of the information and can accept no liability for any loss incurred in any way by any person who may rely on it. You should not act on such information without appropriate professional advice after a thorough examination of the particular situation. Aon reserves the right to change the content of this document at any time without prior notice.

Descriptions, summaries or highlights of coverage do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy. This document has been compiled using information available to us at date of publication.

For further information on our capabilities, please visit: www.aon.co.za or www.aon.com

Aon South Africa Pty Ltd, FSP 20555 | Aon Limpopo Pty Ltd, FSP 12339 | Aon Re Africa Pty Ltd, FSP 20658

October 2025