THE SECURITY CENTRE

Protecting Your World

ARMOUR CYBERSECURITY

WHY SMALL AND MID-SIZED BUSINESSES SHOULD TAKE CYBER THREATS SERIOUSLY

Cyberattacks on small and medium-sized businesses have become increasingly frequent, making it especially crucial for them to prepare.

In an era dominated by digitisation, cybersecurity for small and medium-sized businesses (SMBs) is essential. SMBs are increasingly targets for cybercriminals due to their perceived vulnerability and often inadequate cybersecurity defences. According to a cybercrime study by Accenture, nearly 43% of cyberattacks are on small businesses, but only 14% are prepared.

Overlooking cybersecurity can have devastating consequences, putting revenue, operations, client data and business reputation at risk.

Having worked with many SMBs, these are some of the principal vulnerabilities we have observed.

THE WRONG CYBERSECURITY SOFTWARE

Currently, more than 5,000 types of cybersecurity technologies are available on the market, making it challenging for SMBs to select the right option for their needs. That often leads to uninformed or "easy" decisions that don't offer the best protection to businesses.

LACK OF SPECIALIST SKILLS

It is important to understand that IT and cybersecurity professionals have different skills. We can draw a comparison between a general practitioner and a cardiologist. Would you go to a family doctor to treat complex heart issues? Probably not. It's the same with IT and cybersecurity – while the two functions work side by side, they require distinct training. The lack of qualified people in cybersecurity makes the situation even more complex. This scarcity of talent drives salaries up, meaning smaller businesses often rely on IT generalists to handle their cybersecurity needs, resulting in a higher likelihood of breaches.

THE CHALLENGES OF DIGITAL AND WORKPLACE TRANSFORMATION

Many organisations are moving to the cloud and using web-based software (SaaS) to facilitate hybrid work practices. These solutions are designed to give users accessibility, which translates to hyper-connectivity, which allows cybercriminals to target the digital assets of SMBs from anywhere in the world. The issue becomes even more pronounced as new technologies require a different skill set to secure them effectively, making SMBs relying solely on IT resources especially susceptible.

POTENTIAL THREATS

Cyberattacks are growing in complexity and include everything from ransomware to data breaches and phishing campaigns. Cybercriminals exploit vulnerabilities in outdated software and weak passwords, leveraging stolen credentials and human error. A recent report by the World Economic Forum found that 74% of cybersecurity breaches are attributed to human error, making SMBs without adequate protection easy prey.

UNDERSTANDING THE IMPACTS

The grim reality is that 2023 will be a record year in cybercrime damages, and for SMBs, the costs are high.

Inadequate cybersecurity measures can lead to direct economic losses in ransom payments, data recovery, legal fees, costs associated with prolonged inactivity and regulatory fines. Moreover, the loss of customer trust and reputation damage can have long-lasting financial implications, potentially leading to business closure in extreme cases.

SMBs spend between $826 and $653,587 on cybersecurity incidents. According to Cybersecurity Ventures, in 2023, the cost of cybercrime will hit $8 trillion, growing to $10.5 trillion by 2025.

The value of sensitive data, including customer information, intellectual property, and proprietary business data, cannot be overstated, and a data breach can expose SMBs to significant legal liabilities. Further, a cyberattack that compromises customer data erodes trust and tarnishes reputation, which can be challenging to rebuild.

Cyberattacks often lead to substantial operational disruption. Ransomware attacks, for instance, can render critical systems inaccessible, leading to downtime and lost productivity, usually measured in weeks. The time and resources required to recover from such incidents can be debilitating, with the inability to serve customers or fulfil orders resulting in lost revenue and tainted business relationships.

Finally, governments worldwide have introduced stringent data protection regulations, with one prominent example being the General Data Protection Regulation (GDPR). SMBs are not exempt from such compliance requirements, with non-compliance leading to significant fines.

THE BENEFITS OF ROBUST CYBERSECURITY

SMBs prioritising cybersecurity gain a competitive edge by assuring customers and clients of their data security and integrity commitment, making them more attractive as a business. By contrast, businesses with lax cybersecurity may be perceived as liabilities and excluded from potential collaborations. By prioritising cybersecurity and proactively initiating improvements, SMBs can tip the scale in their favour.

THE ROLE OF PROFESSIONAL CYBERSECURITY SERVICES

In a world where cyber threats are omnipresent, cybersecurity is not an option but an imperative.

There are efficient ways to tap into the cyber services ecosystem, helping right-size the cost while giving you access to world-class expertise and leading technologies, working alongside your in-house IT team.

At The Security Centre, we understand the critical importance of cybersecurity and are committed to safeguarding businesses against threats and vulnerabilities. We believe that a proactive approach to cybersecurity is vital to ensuring cyber resilience and operational continuity.

To better understand the cybersecurity needs of your business, we are offering a **complimentary one-hour assessment and discussion session** with our team of experts, enabling us to address your concerns with tailor-made solutions. To take advantage of this offer, please email **cyber@security.ky**

ABOUT THE AUTHORS

David Chernitzky,
CEO and co-founder
of Armour Cybersecurity

David Chernitzky is a serial entrepreneur and cybersecurity industry veteran, having spent over 12 years working for the Israel Defense Forces and leading IT enterprises worldwide. David helps clients build an accurate big picture of their business and evaluate risks, developing practical mitigation strategies. He has successfully led multiple cyber defence engagements across various industries and geographies and will speak at the Cayman Alternative Investment Summit in January 2024.

Nabeel Yousif,
CIO, The Security Centre

Nabeel Yousif is an award-winning IT executive with a career spanning over two decades, including as a Chief Information Security Officer (CISO) and a Chief Technical Officer (CTO). Nabeel was awarded the 2022 Top 100 CISO award and the prestigious 2023 EC-Council Certified Global CISO Hall of Fame award. He has helped many organisations securely navigate the complexities of the digital world.


THE
SECURITY
CENTRE
Protecting Your World


ARMOUR
CYBERSECURITY