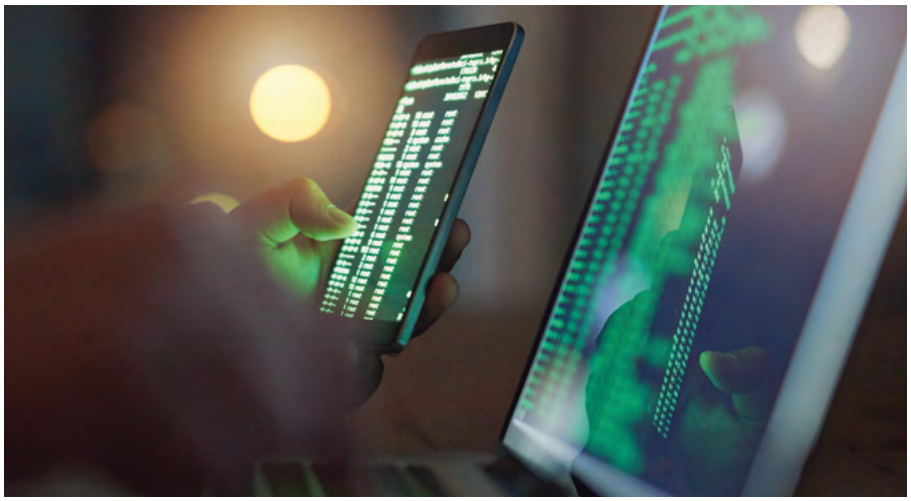
CHUBB®

Cyber-crime

Cyber-crime attacks among smaller and medium-sized companies are on the increase



Cyber-crime is a real and present danger and attacks are becoming increasingly common and more sophisticated, especially among small to medium-sized businesses (SMEs). It is estimated that 32% of South African businesses have experienced cyber-attacks according to the Global Economic Crime Survey (2016) conducted by PWC – on a par with the global average.

Cyber security is uniquely challenging for SMEs, due to a combination of the frequency with which these threats become bona fide cyber security incidents, the severe business disruption and financial impact, and limited resources to respond and recover in the event of an attack.

Jenny Jooste, Professional Indemnity and Cyber Underwriter at Chubb Insurance South Africa, says: "Our claims data and global research is showing that cyberattacks directed at SMEs are steadily increasing. As a group, SMEs tend to devote inadequate resources, time and funds to cybersecurity with fewer than 3% of all SMEs having cyber insurance. Criminals target these companies because their IT controls are not as sophisticated as large corporate companies, and the skills for dealing with these threats are often not specialised, making them perfect targets."

According to Jenny, cyber criminals typically look for targets that can be hacked with ease. "They often accomplish this by using software that automatically scans the web and identifies businesses with specific security weaknesses such as outdated or unpatched software, poor password hygiene, open web ports, unencrypted data in transit, lacking endpoint protection and the like. They can also gain entry through a server room break-in or from internal network hacking, which then enables monitoring by criminal third parties. This can often be triggered by something as innocuous as plugging an infected USB drive into a computer or device that is connected to an internal network."

She also raised the issue of liability relating to cyber exposure, which company directors ignore at their peril.

"Directors and officers can be held liable in their personal capacity for their fiduciary duties should the necessary measures and policies not be in place to mitigate cyber liability exposure for the company. Claiming ignorance about cyber risks is no longer an excuse, and proactive steps must take centre stage to mitigate and prepare for potential cyber threats, no matter the size of your business," warns Jenny.

How can SMEs protect themselves from cyberattacks?

Although stopping cyber criminals from accessing data may seem like a formidable task, there are simple measures that companies can use to create their own cyber risk management program and limit their exposure. Chubb Insurance provides the following important tips:

- **Focus on the basics**
  Ensure that antivirus, firewalls, patches and other security software is always up to date. Also ask a cybersecurity consultant to identify high risk areas and address these.
  - Does IT know at which point you want to be alerted regarding a breach?
  - Do you have a specific person with responsibility for Information Security (IS)?
  - Is there a formal IS policy in place? How often is it reviewed and by who? Are recommendations acted upon?
  - Have you implemented user security awareness training? How often? How relevant is it to your business?
  - Is an audit report done on potential areas of risk on operational (non-financial) systems?
  - Is someone tracking the evolving cyber-regulatory environment?
  - Will someone monitor decisions made by regulators in response to cyber incidents?
  - Do you have an appropriate cyber insurance programme in place and do you know how it will work?
  - Is your data encrypted?
  - Is IT conducting forensic readiness assessments?
  - Are incident response plans being tested?
  - Has the quality of the back-ups been tested?
  - Are effective "real-time" monitoring processes in place?
  - Is the type of data and the impact of breach understood? Have you identified critical information security risks and put in place appropriate monitoring and controls?

- Have information resources been classified according to sensitivity and criticality? Have corresponding levels of security been implemented?
- Is dual authentication required for access to critical Information Systems?
- Are users required to regularly update passwords? Criteria?
- Are laptops protected by personal firewalls?
- Is antivirus software installed on ALL systems and are updates monitored?

- **Educate all employees regularly on cybersecurity vigilance**
  Employees should be aware of the role they play in preventing a cyber breach, especially when company laptops or other devices are used offsite. They should gain access via VPN sign on procedures and never use USBs. Establish positive and secure habits with regularly scheduled training and education by empowering the IT department to send regular "tester emails" to staff to see who can identify phishing emails. This training needs to be ongoing. Some basic clues that indicate phishing:
  1. Enticing: Offers that are too good to be true
  2. Urgent: Pressure tactics such as threats, rushing or name dropping
  3. Unsolicited: Contact is unexpected or not from someone you would expect e.g. CEO.
  4. Odd: The tone is off, especially from a colleague or friend.
  5. Unknown: Unknown requester, email address doesn't match the message e.g. someone@gmail from UPS, the URL isn't correctly (AmericExpress.com)
  6. Sloppy: Spelling or grammatical mistakes, branding is old or unusual.
  7. Unusual: Requests are outside normal procedures or break of normal policy

- **Develop and enforce a formal, written password policy**
  Establish a written password policy requiring strong passwords such as a mix of letters, numbers and symbols that are frequently changed. Passwords should also be changed and user portfolios marked as inactive when employees leave the company.

- **Update IT equipment and deploy security software**
  Outdated operating systems and computers are inherently more vulnerable to more sophisticated hacking techniques and newer forms of malware. It is also important to monitor those who have legitimate access to the network as well as monitoring the network itself to highlight abnormal activities. Basic downloadable software offerings are available to SMEs and can be operational within minutes.

- **Create a cyber incident response plan**
  Less damaging incidents can be resolved with a dedicated and prepared team of cyber responders that may comprise of employees and outside service providers. It will provide a shorter response time and a quicker resolution to the issue, if it is within the means of the team.

- **Put a disaster recovery plan in place**
  Typically, disaster recovery planning involves analysis of business processes and continuity needs that are required so that an organisation can continue to operate, even if it is offsite from a different location. Make sure a copy of the plan is printed for staff use because if your system is hacked, you won't be able to get your plan from your PC.

- **Purchase cyber insurance**
  After getting all IT control measures in place, ensure that you investigate purchasing a cyber liability insurance policy, which covers first and third-party liability. The cost of this will always be far less than the cost of shutting down a business in the wake of a cyberattack.

"It is evident that the threat of cyber-crime is not going away anytime soon and the cost of a breach can be crippling to a small business. Businesses that embrace the necessary safeguards, together with other measures outlined by their insurer and broker are putting themselves in a strong reactive position to recover with their bottom line and reputation intact," concludes Jenny.

Get in touch

Additional information can be found at:
www.chubb.com/za