STORMGuidance

2021 Report: Impact of Cybercrime on SMEs in South Africa

stormguidance.com
contact@stormguidance.com

Cybercriminals and technologies are continuously learning and evolving

Globally, we must challenge this growing threat landscape, assess our cyber risk maturity, plan for the best response to cyber incidents and implement measures to coordinate immediate recovery in the event of a cyberattack.

This is precisely what STORM Guidance do; **Assess, Plan,** and **Respond.**

STORM provides a comprehensive suite of specialist advisory services which help clients to understand their information risks. They devise plans for managing cyber incidents and assist in coordinating the response to incidents when they occur using digital investigations and advanced recovery techniques. STORM specialists have helped hundreds of clients recover from a range of cyber incidents, including Ransomware, Business Email Compromise (BEC), Extortion and Data Theft.

CyberCare is an incident response service that has been developed by STORM Guidance. In May 2021, access to membership was extended to South African organisations enabling a fresh approach to tackling cybercrime in the region.

Created to give business groups and their members the best chance to investigate and recover from a cyber incident, the service offers access to the world's best cyber triage and response specialists, whilst also protecting its constituents against high incident response fees. CyberCare cover includes technical triage, specialist support for existing IT, and computer forensic investigation.

Foreword

“Even after decades of experience in cyber risk and investigations, I am always really interested in developing a picture of cyber risk and asking membership organisations to respond to this. Our first such survey in South Africa, has revealed some key learning, particularly in the perception of cybercrime and how it is affecting businesses across many sectors.

The overriding message from the survey responses has been that member organisations and their constituents recognise cyber risk as being paramount on their list of management concerns. However, perhaps one thing that enhances this concern even further is how they measure and manage such risk. One especially important aspect of this risk is how members will respond to cyber incidents when they occur!

Most businesses have not considered this critical question and expecting their IT provider or law enforcement to help them in such circumstances will likely lead to considerable unnecessary loss and disappointment.

Helping organisations deal with this risk is why we have created our CyberCare cyber incident response hotline service for South African SMEs. We look forward to serving clients with a range of options for both IT and senior management, in the investigation and recovery of their business from potentially damaging cyber incidents.”

Neil Hare-Brown

CEO STORM Guidance

Executive summary

The 2021 STORM Guidance survey of businesses in South Africa addressed the growing concerns over increasing cyber threat in the region

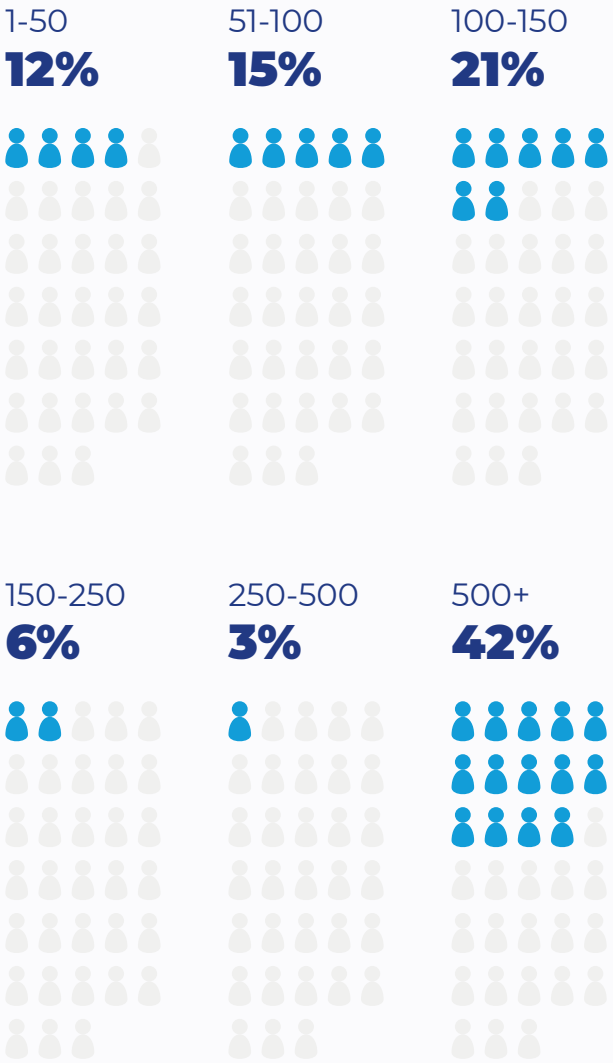
The survey, conducted in May, examined 33 business groups across the country, representing approximately 10’000 SMEs, giving an insightful panorama of the issues at hand.

An alarming 43% of cyberattacks target small businesses, particularly those in the financial, health care, retail, insurance, and legal sectors; cybercrime is evidently not just a large business issue. To delve a little deeper, key sectors in technology, utilities, and materials are just part of a cyber exposure picture that is costing businesses over R2.2 billion every year. With SA falling victim to the third-highest number of cyberattacks of any country, it was time the situation was investigated.

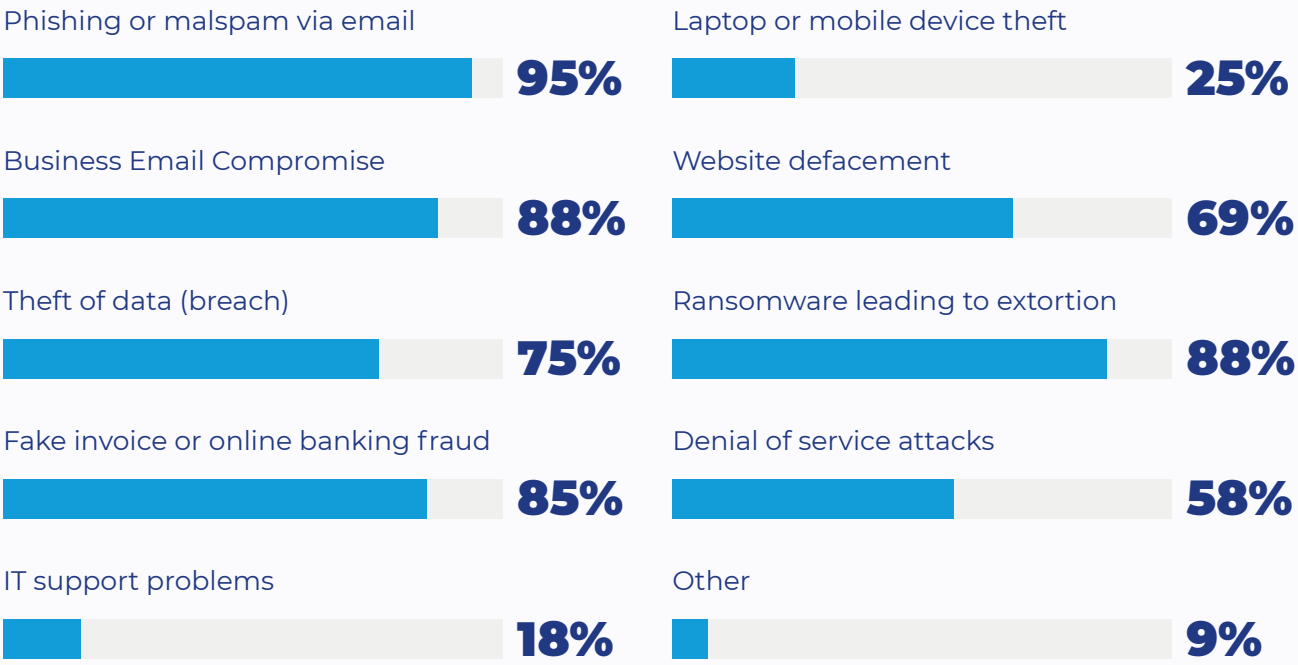
The survey was completed by 33 business groups who represented between 1 – 50, and 500+ business members each. The report’s findings are outlined below.

How many members does your organisation have?

33 businesses responded. The following charts represent the size of each group



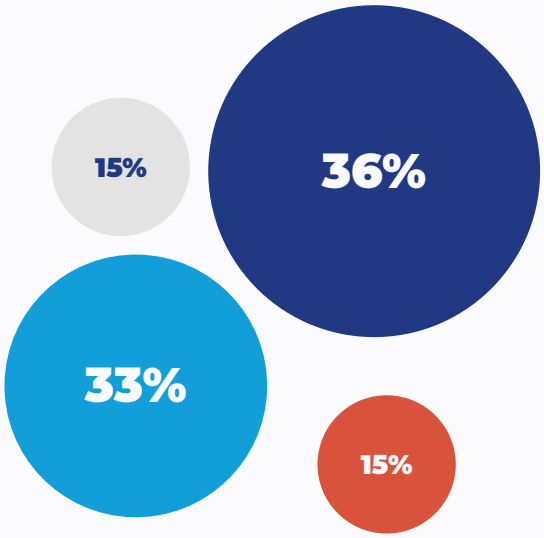
How would you define cybercrime?



Assessing the general understanding of the topic, the STORM Guidance survey found that almost all respondents (31) identified 'Phishing or Malspam via email' as an incident which is actually a pre-cursor to a cyber-attack.

This was closely followed by 'Business Email Compromise (BEC)' and 'Ransomware'. Although reassurance can be taken from some understanding here, it must also be noted that almost a quarter of the respondents answered, 'laptop or mobile device theft', and as many as 6 business groups chose 'IT support problems'. It would be fair to say that more work is needed in the education and awareness of cyber risk in the workplace.

Do you consider cybercrime to be a problem for small and medium sized businesses in South Africa?

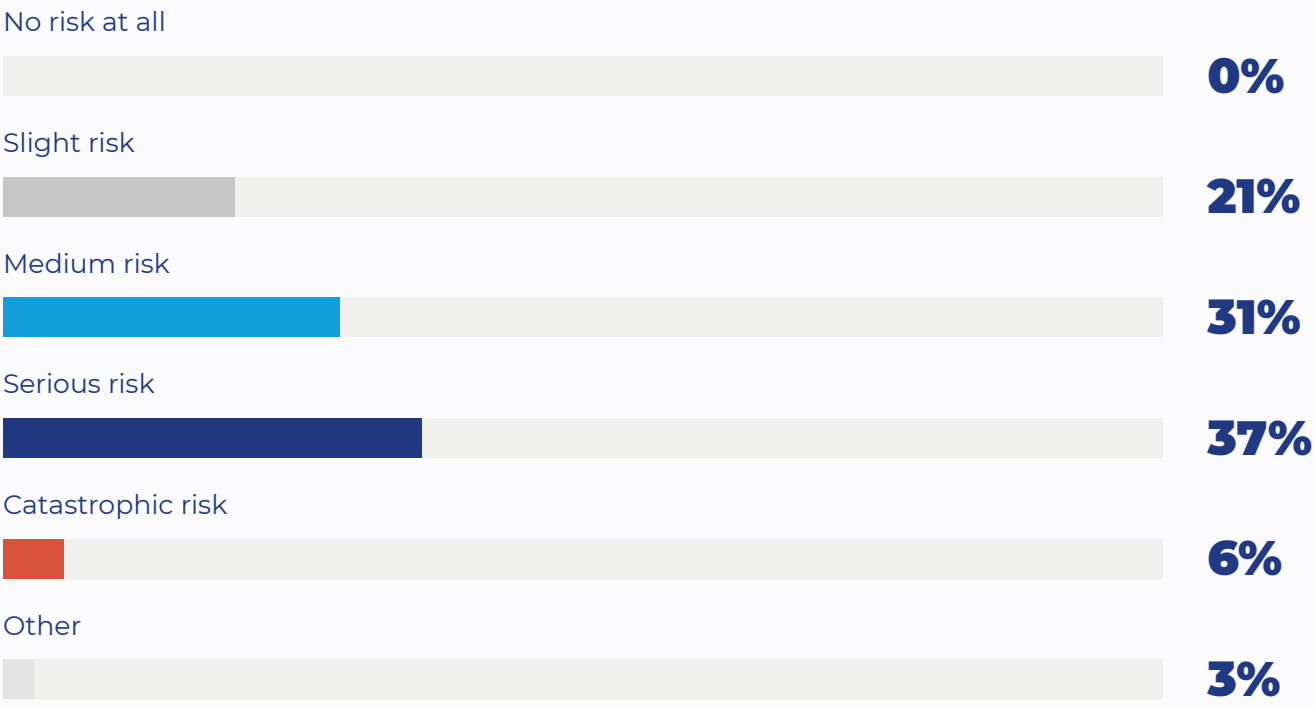


28 of the 33 respondents see cyber risk as a definite, significant, or extremely serious problem.

This clearly illustrates concerns across the board with only 5 business groups that considered cybercrime to be only 'somewhat of a problem'.

- Somewhat of a problem
- Definitely a problem
- Significant problem
- Extremely serious problem

Rate the cybercrime risk level that your members are exposed to

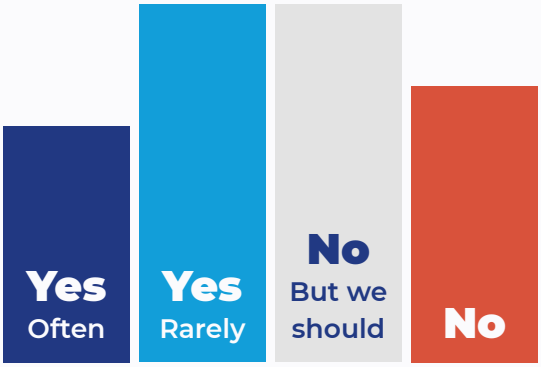


One-third of the business groups surveyed expressed the level of cybercrime risk that their members are exposed to as being **serious.**

Two respondents considered the risk to their organisations; should it be realised, at a **catastrophic** level.

25 of the 33 business groups considered cybercrime as either a **medium risk** or of greater severity.

Have your members reported or discussed cybercrime with you?



To determine a true measure of those who have been directly affected by cybercrime, the survey asked if members had reported or discussed cybercrime with their business group.

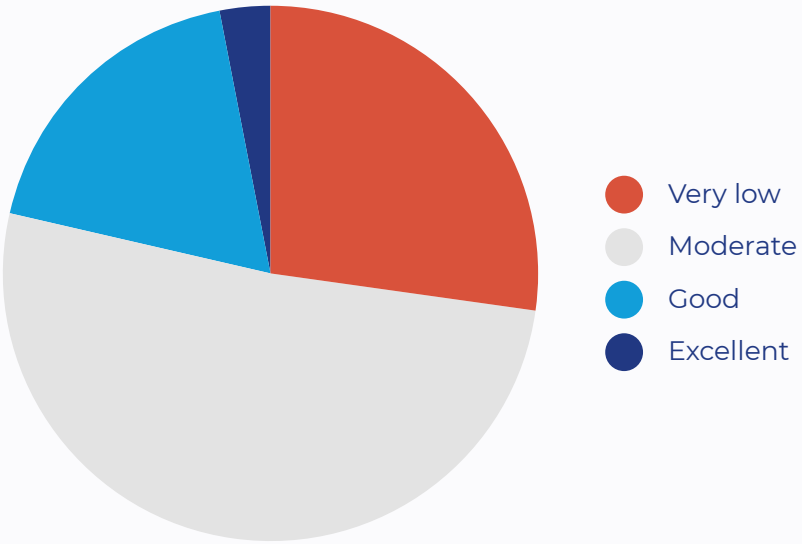
7 business groups answered 'yes – often', 9 reported 'yes – rarely', a further 9 declared 'no – but we should'. Further, 8 business groups responded that their members have not reported or discussed cybercrime with them.

Although this could be seen as a measure of those who have been affected by cybercrime, it could also reflect how willing SMEs are to report incidents when they occur and to the ability of the business groups to learn of such incidents.

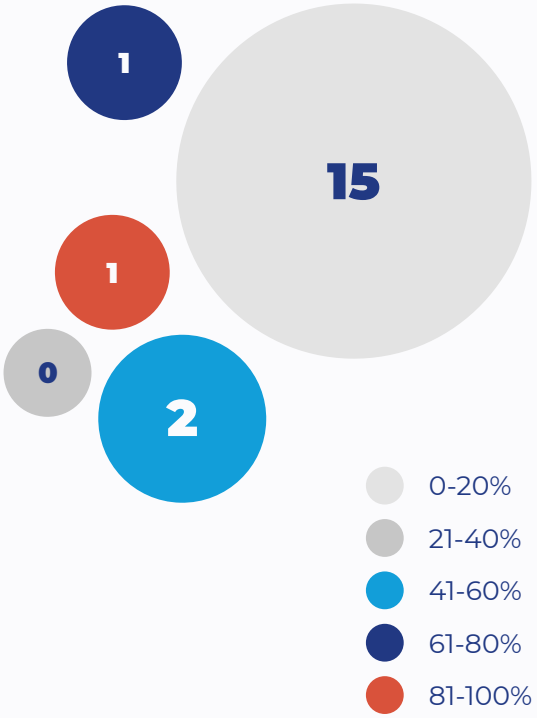
What do you consider the general level of cybersecurity to be across your membership?

Taking a closer look at the level of cybersecurity maturity across business group members, the survey sought to determine what business groups perceived this to be.

9 of the 33 respondents declared it to be ‘very low’, 17 answered ‘moderate’, a further 6 stated they considered it to be ‘good’, with just one business group estimating their members to have an ‘excellent’ level of cybersecurity. This clearly indicated a general low level of effective cyber risk management capability, and that business groups have some work to do to ensure members cyber resilience does not unduly expose their businesses.



As a percentage, how many of your members have suffered a cybercrime in the last 12 months?



In the hope of transparency between members and their business groups, the survey looked to determine how many business group members had suffered a cybercrime in the last 12 months.

Almost half of the respondents were unable or unwilling to answer, whilst a third claimed the figure to be above 10% of their members. Some went so far as to claim that as many as 50%, 65%, and 90% of their members had suffered a cyberattack in the last 12 months.

Rate the impact that a cybercrime incident would have on your members?

SMEs should consider the impact a cyberattack would have on their business and operations, to prioritise better preparedness in the event of an incident.

When asked to rate the impact a cybercrime incident would have on members, each business group answered with a reflection of how ready they interpret their members to be in the event of a cyberattack. Just under 60% said a cyberattack would have a high impact on their members, while just 5 business groups expressed minimal concern.

Severe impact

Potentially threatening continuation of business

High impact

But capable of being absorbed on balance sheet

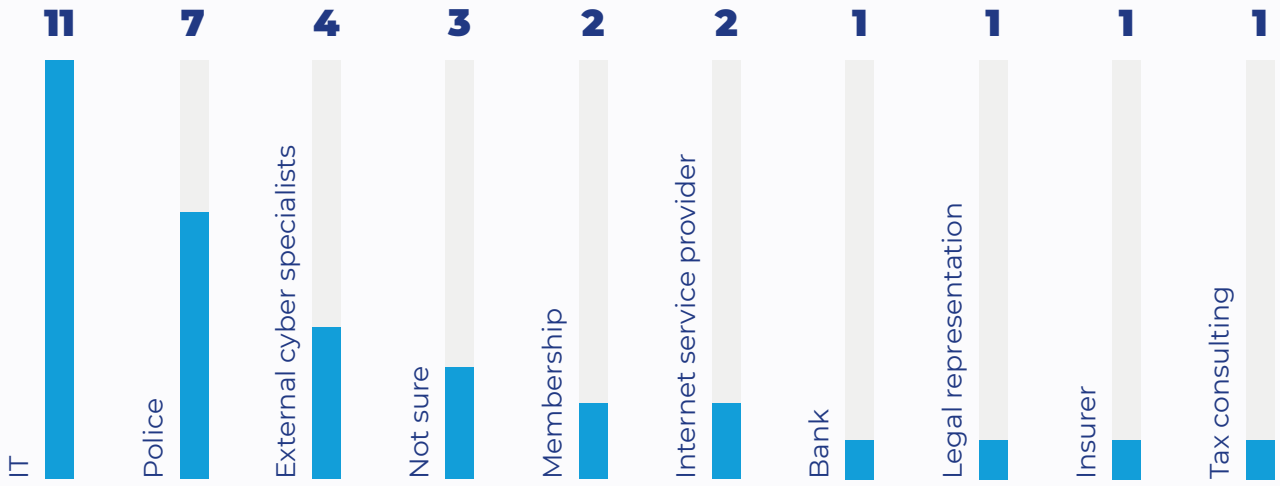
Medium impact

Some financial/ operational loss or possible reputational harm

Low impact

Negligible financial/ operational loss

Who do you think your members would contact for help if they fell victim to cybercrime?



The survey asked respondents who they expected their members would call in the event of a cyber incident.

A third of those asked said that they would contact IT support, and following closely behind, the Police (7) were named as the first point of call.

Whilst law enforcement is involved in dealing with cybercrime, the expectations victims have for immediate response is unrealistic. Whilst the police should always be considered in reporting cybercrime, they are generally not resourced to help organisations when it comes to thorough individual investigations, identifying vulnerabilities, and resecuring systems to prevent reoccurrence.

Conclusion

It is hoped that the recent launch of CyberCare in South Africa will go some way to address the concerns in the findings of this survey and those raised by the respondents in their answers.

Business groups whose members use the service will be offering access to some of the world's leading cyber incident response professionals to assist members in both thorough and confidential investigation and recovery from cyber incidents.

However, more is needed to tackle the issues faced by South African Businesses. It is essential to introduce cybersecurity training to the workplace, and even the classroom, to help organisations to address the skills gap. Businesses must attend to the lack of sufficient IT security budgets and make efforts to keep abreast of cyberthreats. More onus is needed on African governments to look into a long-term strategy that identifies the problem at its root and help SA businesses to stay resilient.