# Board level strategies for effective cyber risk management

## LSSA Collaborative partner: Storm Guidance

Cyber extortion has become a hot topic across all industry sectors, as cyberattacks now hit the news daily. The global cybercrime pandemic has revealed huge spikes in data theft and businesses held to ransom, and the legal sector is no exception. Law firms are valuable targets to threat actors due to the enticing value of the financial gains resulting from interception and diversion of client funds or through extortion in the immediate wake of data breaches and ransomware infections.

Such attacks on the legal sector are increasingly sophisticated involving a great deal of research and planning by the cybercriminals who know that such investment is more likely to yield results. To put this into perspective, the UK Solicitors Regulation Authority revealed a 300% increase in phishing scams in the first two months of lockdown alone. This is more than three times the amount reported during the same timescale in 2019.

### But how are things looking for South African law firms?

The Legal Practitioners' Indemnity Insurance Fund NPC (LPIIF), report that South African law firms have been the target of cybercriminals for over a decade and conveyancing attorneys specifically are a major target of threat actors and bear the brunt of the bulk of these cyberattacks. The High Court case of Fourie v Van der Spuy and De Jongh Inc. demonstrated that the courts are not sympathetic to practitioners who have failed to take adequate steps to prevent or mitigate a successful cyberattack.

More recently, the introduction of the Protection of Personal Information Act (POPIA) in South Africa on July 1st of this year, legislates the protection of personal information processed by public and private bodies. POPIA outlines the rights of data subjects, regulates cross-border flow of personal information, mandates security over personal data, introduces mandatory obligations to report and notify data breach incidents, and imposes statutory penalties for violations of the law.

For South African law firms concerned with the increasing threat that cybercriminals pose to their firms and their clients, and about the new levels of accountability brought about by the introduction of POPIA, it is imperative to act now to implement security measures to mitigate cyber risk and prepare for the increasingly likely cyber incident.

### Global findings and outlook.

Firms are increasingly concerned about the potential for increased vulnerability brought on by the shift to remote working since COVID-19, with unpatched personal IoT devices and internet connections failing miserably to protect business networks and data against malicious activity. Further, after the rollout of 5G's increasing bandwidths, IoT devices are now more vulnerable to cyberattacks than ever before.

According to an article by Forbes, the state of our cybersecurity readiness is alarming, and the following stats are a testament to our global failings.

> On average, only 5% of companies' folders are properly protected - 2019 Global Data Risk Report | Varonis
>
> Cybercrime will cost the world $10.5 trillion annually by 2025 - The Evil Internet Minute 2019 | RiskIQ

The average cost of a data breach is $3.86 million as of 2020 - Data Breach Costs: Calculating the Losses for Security and IT Pros (dice.com)

Malware increased by 358% in 2020 – Help Net Security

Phishing attacks account for more than 80% of reported security incidents – CSO Online

There was a ransomware victim every 10 seconds in 2020 – Infosecurity Magazine

Netscout threat intelligence saw 4.83 million DDoS attacks in 1H 2020 - This is roughly 26,000 attacks a day or 18 attacks per minute. - NETSCOUT Threat Intelligence Report Findings from 1H 2020

Nearly 80% of senior IT and IT security leaders believe their organisations lack sufficient protection against cyberattacks despite increased IT security investments made in 2020 to deal with distributed IT and work-from-home challenges, according to a new IDG Research Services survey commissioned by Insight Enterprises.

## What measures should firms take to reduce their cyber risks?

If 2020/21 has taught us anything, it is that the cybersecurity skills gap is one of the greatest issues faced by organisations globally, and it is time this is addressed at board level across all industry sectors. With many senior partners raising the question over whether their organisation is adequately protected against cyberthreat, board members are requesting non-technical lists of what is needed to manage their cyber risk effectively.

Traditionally seen as the sole responsibility of IT and security roles within a firm, cybersecurity positioning must now be translatable to boards, with strategies that need to be adopted to better manage cyber risk.

> *In order to manage cyber risk effectively, boards need to understand, implement and monitor key strategies. They should not be concerned with tactical and operational level controls which, whilst also vitally important, use technical jargon which takes years of subject matter experience to understand and master. The challenge is not to train board executives to understand the technicalities, it is for boards to understand and master the strategies needed to support effective cyber risk management.* - **Neil Hare-Brown – CEO STORM Guidance** - March 2019 Governance Issue 295

In view of opening discussion at board level, it is time we engage partners and executives with useful, strategic thinking using business language.

STORM's CyberSeven framework was created as a foundational review which identifies the seven key strategies that are necessary for any organisation to manage cyber risk effectively.

Today it has become apparent that effective cyber risk management and resilience involves various protections, and not just technology. High-level sponsorship, budgeting, staff resourcing, specialist skills, staff awareness, control over payments and cyber insurance are all equally as important in enabling mature cyber risk resilience.

These protections are often overseen by business and board leaders, and so it is important that these key strategies are translatable to the very partners and executives who make high-level decisions.

## CyberSeven key review areas.

**Responsibilities**

Having clearly defined roles for reporting cybersecurity to key executives guarantees an organisation will be sufficiently sighted on risks. CyberSeven identifies the assignment of critical board responsibilities.

**Asset awareness**

Maintaining a register of data assets is a crucial step in defining your approach to cybersecurity. The review assesses the value of the intangible assets you control and their impact on your cyber risk profile.

**IT budget**

Cybercriminals find little resistance when it comes to organisations with underfunded IT teams and infrastructure. CyberSeven assesses the level of funding dedicated to IT and cybersecurity.

**Payment controls**

Fraud is countered by segregating payment duties, defining processes for payment detail changes, and auditing automated payments. The review focuses on the segmentation of your payment functions to prevent fraud.

**IT staff count ratio**

An under-resourced IT department handling too many responsibilities will lead to disaster. CyberSeven assesses the adequacy of resourcing to manage IT and security effectively.

**Cyber skills and awareness**

A culture of security awareness supported by training ensures that employees are vigilant defenders of company assets. The review assesses the maintenance of your staff's capabilities and vigilance.

**Technology versions**

Ensuring the security of technologies that you and your vendors use will result in criminals perceiving your business as a hard target. CyberSeven assesses your technology strategy to stay ahead of cybercriminals.

The CyberSeven strategies were identified over many years of assessing the common shortcomings in organisations that have suffered a cyber incident. By collecting key observational data across hundreds of cyber incidents, our team has used its decades of experience in cyber risk management and has helped thousands of businesses recover from cyberattacks.

Whilst we appreciate that cybersecurity is a highly technical area, it is more important now than ever before that the subject is overseen and tackled at board level and that partners and executives are engaged and informed on cyber risk management. With a business-aligned and jargon-less set of strategies in place, organisations can work collaboratively in the fight against the global, increasingly sophisticated, cybercrime pandemic.

*'There must be a challenge to the current status quo. Boardrooms have become over-reliant on technical teams for advice and, as a result, restricted in how they can manage cyber risk from a strategic level. If controls are maintained only at operational level with no foundational strategy to maintain them, then the overall cyber resilience is likely to be flawed.'* – **Neil Hare-Brown**

## '*Tactics without strategy is the noise before defeat*' – Sun Tzu, The Art of War

We have developed the above strategies into a 30-minute self-assessment, to learn more go to https://www.cyberseven.global/. LSSA members can get access for free by emailing contact@stormguidance.com.