DATA BREACHES IN SOUTH AFRICA: SURVEY REPORT

Author: Homba Ngejane

SUMMARY

As security breaches continue to escalate, security professionals urgently require actionable data to make informed decisions for their organisations. To address this need, we conducted a comprehensive survey involving 309 respondents from various provinces of South Africa. The sample included officials from diverse sectors, such as public, private, nonprofit and small, medium and micro enterprises. Participants held positions including executives, directors, managers, or contributors in fields like information technology, cybersecurity, software development and DevOps, with direct or indirect responsibility for cybersecurity.

The objective of the survey was to provide a detailed overview of the cyberattack landscape facing South African organisations. We examined how organisations are breached, the initial causes of attacks, resolution times and the financial impact associated with these incidents. Our key finding will assist security professionals and leaders develop informed, strategic responses to cyber incidents.

The following section presents data analysis and key insights based on the types of cyberattacks experienced, methods used, impact on the information technology (IT) infrastructure and techniques used to mitigate, prevent or remediate these attacks.

DATA ANALYSIS AND KEY FINDINGS

FREQUENCY OF BREACHES OVER 12 MONTHS

Figure 1 shows the frequency of breaches in the last 12 months. About 88% of the participants admitted to having suffered a security breach. Of these, 90% of those were targeted multiple times. This can imply that a successful initial attack increases the likelihood of subsequent attacks on the same organisation's infrastructure. Those who reported "none" did not mention their preventative, mitigation and remediation measures compared to those who had been compromised. These organisations may either be exceptionally secure or possibly unaware of events occurring. In future surveys, it might be useful to ask if new activities or systems were implemented as a direct result of a specific or series of breaches.

NUMBER OF BREACHES OVER THE LAST 12 MONTHS

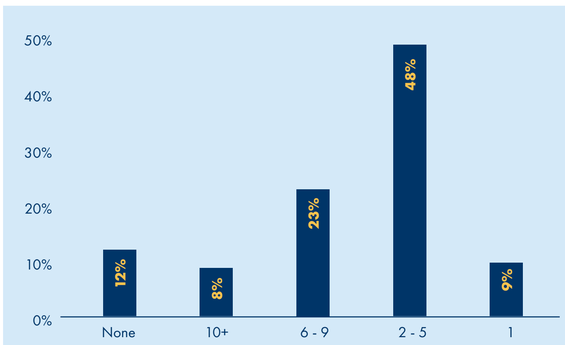

Figure 1: Number of incidents experienced in the past 12 months

TYPE OF CYBER BREACH EXPERIENCED

As shown in Figure 2, the top three cyberattacks facing organisations were Malware (65%), which is the most commonly mentioned incident by organisations, with just over half (55%) reporting application attacks and the third experiencing insider threats (30%). Other attacks reported by less than 30% included crypto-jacking/crypto-mining, wiper attacks, ransomware and the lowest number of incidents (8%) were out down to DDos. In summary, almost 87.8% of organisations experienced at least one type of cyber incident in the past 12 months and one-third (35.3%) had experienced 3 or more incidents.

TYPES OF CYBERATTACKS EXPERIENCED

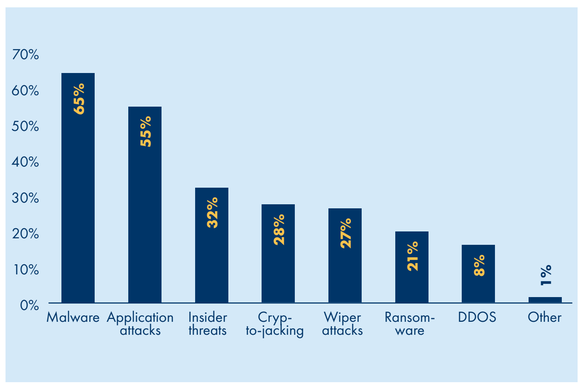

Figure 2: Types of cyberattack experienced

ROOT CAUSE

The main root cause listed was third-party connections to the enterprise at (48%), with similar proportions stating that it was phishing (45%) or hardware-based attacks (43.0%), as shown in Figure 3. Less frequently mentioned causes were supply chain attacks through SaaS, DevOps Depos (e.g. GitHub) and the least (9%) reported IOT. Organisations gave different root causes for the same attack, sometimes giving more than one reason for the incident. It was not possible to link the cause with the type of attack where more than one was mentioned

SOURCE OF THE BREACH

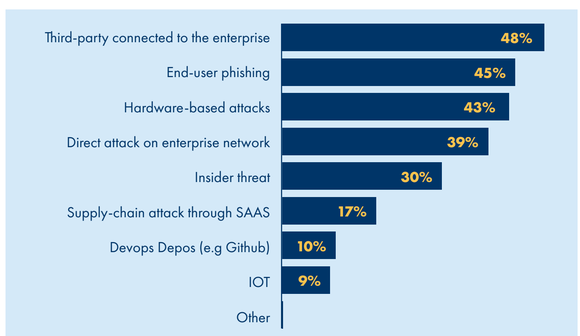

Figure 3: Source of the cyberattack

IMPACT

In terms of impact, this study sought to understand the damage to infrastructure, financial loss associated with the attack, the time it took the organisation to resolve the issue and data loss, particularly personally identifiable information (PII). Overall, three-quarters reported a low to moderate impact (78%), with only 4% reporting a very high impact (Figure 4). Although it was not possible to link the exact type of incident with impact, it was noted that fewer incidents were related to a lower impact. However, some organisations mentioned that in some cases, only one event caused a very high impact.

OVERALL IMPACT PER FREQUENCY OF THE ATTACK

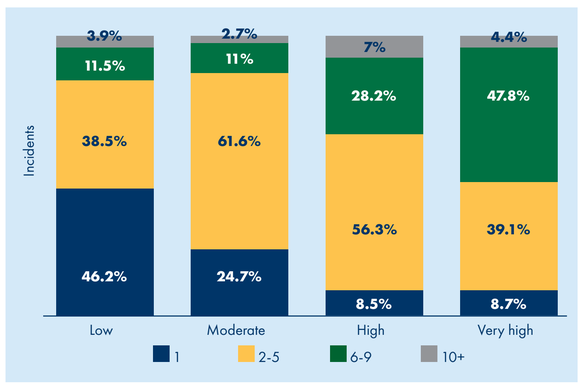

Figure 4: Overall impact of cyber-incidents on organisations

RECOVERY

Figure 5 shows that most low-impact incidents took hours to resolve, but this proportion was reduced by almost half to 45.5% in the case of high-impact incidents. Over a quarter of the organisations reported that it took months to recover from very high-impact circumstances. It was also discovered that many of those reporting months of recovery had commonly experienced denial-of-service attacks.

OVERALL IMPACT

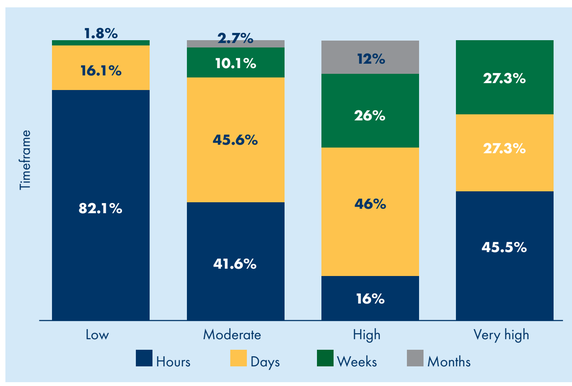

Figure 5: Recovery time according to the impact of the incident

FINANCIAL LOSS

The monetary value incurred due to the attack was correlated with the disruption caused to the organisation, where shorter disruptions generally incurred lower costs, with only (3%) incurring over a million rands as a result of the breach (Figure 6). However, there were exceptions where brief disruptions resulted in substantial expenses. It is also important to note that financial loss could have been influenced by other factors such as fines, hiring service providers, or loss of business profits due to disruptions.

FINANCIAL COST

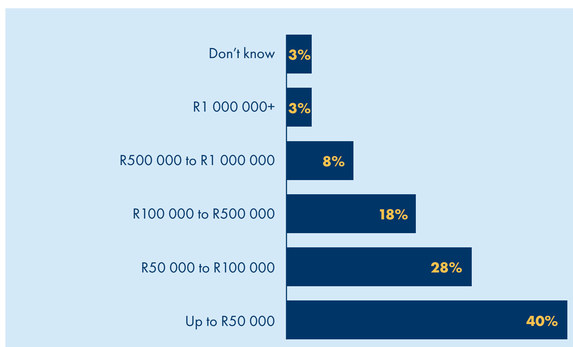

Figure 6: Financial cost

DATA LOSS

Lastly, on impact, Figure 7 shows that about (42%) experienced data loss, particularly PII records, due to the attack, while the rest (58) indicated that the impact of the attack did not result in any loss of such records.

DATA LOSS

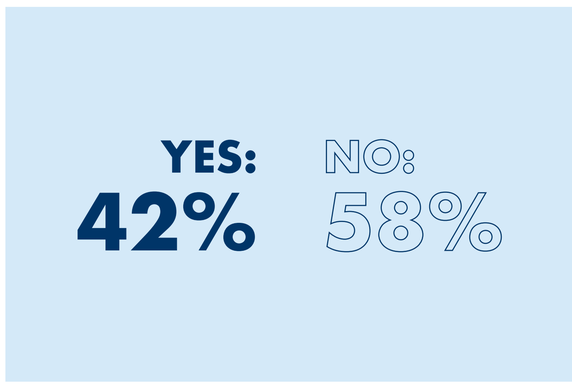

Figure 7: Data loss (PII) due to cyberattacks

CYBERATTACK MITIGATION, REMEDIATION AND PREVENTION

For cyberattack mitigation, remediation and prevention strategies, this study looked at three components: security practices for mitigation, remediation solutions and offensive strategies. Accordingly, respondents put forward a range of security practices for cyberattack mitigation. As shown in Figure 8, the most common response (71%) for security practices by these organisations was multifactor authentication adoption. With approximately half reporting moving Exchange to Cloud/ Managed (52%), application security in CI/CD pipelines (50%) and corporate phishing and awareness campaigns (49%). A quarter or less mentioned hiring MSSP to offload activities (26%), and the least privileges adoption (20%). All organisations reported at least one practice and most organisations (83.2%) implemented at least two practices.

MITIGATION SECURITY PRACTICES

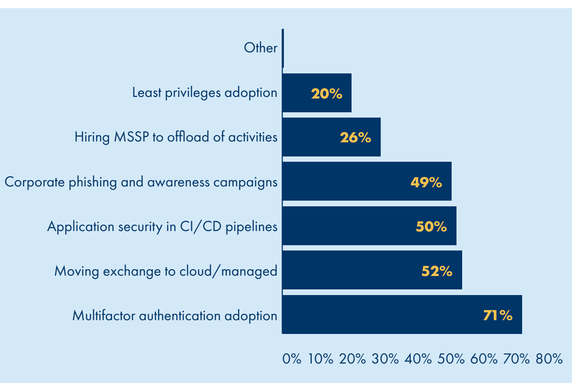

Figure 8: Mitigation strategies

For remediation solutions, Figure 9 shows that Web application and API protection were the most commonly mentioned (64%), followed by identity access management and web security gateways (both 58%). Half or fewer stated disaster recovery/backup protection, software-defined segmentation and cloud posture management solutions. The lowest reported solution was EDR (11%). In addition, almost all (87.8%) organisations mentioned at least one solution, with 10.2% reporting six or more.

REMEDIATION SOLUTIONS

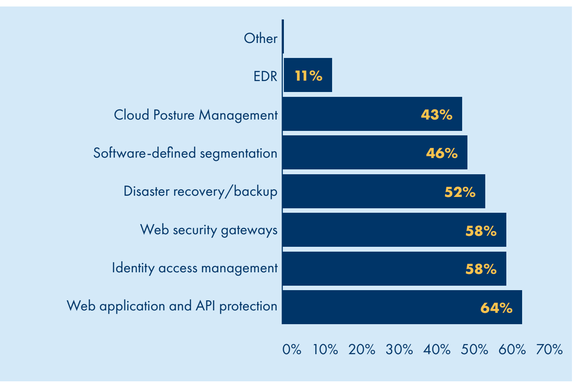

Figure 9: Remediation solutions

Lastly, for preventative measures, as shown in Figure 10, organisations were asked about the offensive techniques currently in use. Over half (56%) employed attack surface management, followed by a half (50%) or less using third-party pen testing, breach attack simulation, in-house pen testing/red team and continuous automated red teaming. The least used technique reported (17%) was purple teaming. Three-quarters of the organisations (75.9%) used at least two of these solutions.

PREVENTATIVE MEASURES

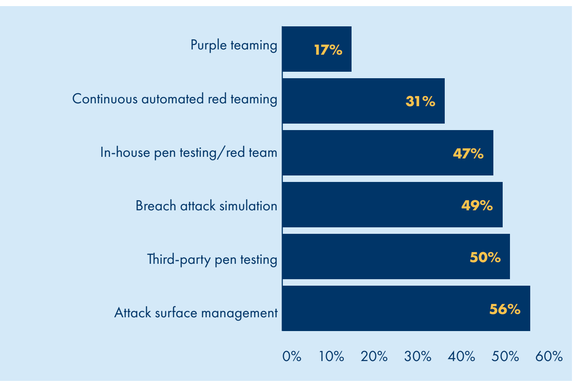

Figure 10: Offensive techniques

CONCLUDING REMARKS

The report highlights the most commonly exploited attack vectors by malicious actors and examines the consequences these breaches had on the IT infrastructure. It is important to note that the majority of organisations operated in the private or public sector (91%), while other sectors were not well represented (nonprofit, small and medium enterprise, parastatal and others). Moreover, only three provinces were well presented in the data analysis (i.e. Gauteng, the Western Cape and KwaZulu-Natal), potentially due to the digital divide, as the other provinces are predominantly rural.

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

For more information, visit **www.csir.co.za**

CSIR
Touching lives through innovation