Data Breaches

The unseen iceberg in the cyber sea

June 2022 Newsletter

18th Edition

RMG

Table of Contents

A physical breach involves the physical theft of documents or equipment containing information that hackers are not authorised to have in their possession.

Electronic data breaches occur when a hacker gains unauthorised access to a system or network environment where personal and financial details are stored, processed, or transmitted.

Skimming involves an external device that is installed on a merchant's point of sale device without their knowledge.

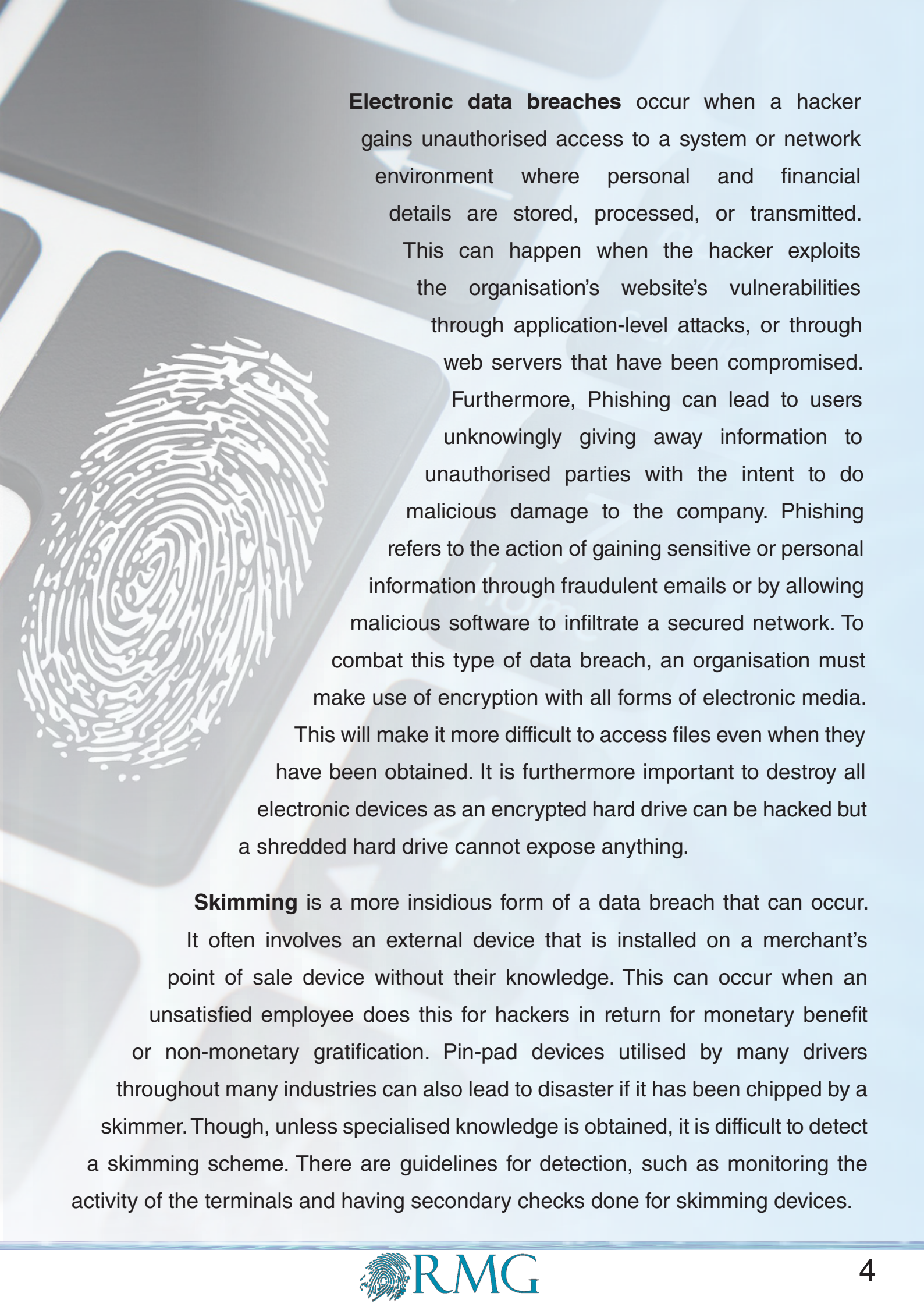
What is a data breach?

A data breach is an incident where information is stolen or taken from a system or person without the knowledge, nor with the authorisation of the owner of the system. As most hackers intend to get personal information of data subjects, all organisations are at risk of experiencing data breaches in some form at some stage. ShredNations establishes a framework of three main data breach types. All three types share the same amount of risk and consequences to the business, but they are unique in their execution. Even simple tasks such as document shredding can become a prevalent factor that can save a company from a potentially fatal data breach.

A data breach is an incident where information is stolen or taken from a system or person without the knowledge, nor with the authorisation of the owner of the system.

Types of Data Breaches

A **physical breach** involves the physical theft of documents or equipment containing information that hackers are not authorised to have in their possession. This type of data breach involves corporate espionage and focuses on risky items that store information. This can include laptops, desktop computers, hard drives, and point-of-sale equipment. Preventing this type of breach can be attained using security and access control measures. Always remember to destroy devices once they are no longer in use, forgotten hard drives and old computers that pile up are ripe fruit for hackers to pick, and in most circumstances, no one will notice that they have gone missing.



Electronic data breaches occur when a hacker gains unauthorised access to a system or network environment where personal and financial details are stored, processed, or transmitted. This can happen when the hacker exploits the organisation's website's vulnerabilities through application-level attacks, or through web servers that have been compromised. Furthermore, Phishing can lead to users unknowingly giving away information to unauthorised parties with the intent to do malicious damage to the company. Phishing refers to the action of gaining sensitive or personal information through fraudulent emails or by allowing malicious software to infiltrate a secured network. To combat this type of data breach, an organisation must make use of encryption with all forms of electronic media. This will make it more difficult to access files even when they have been obtained. It is furthermore important to destroy all electronic devices as an encrypted hard drive can be hacked but a shredded hard drive cannot expose anything.

Skimming is a more insidious form of a data breach that can occur. It often involves an external device that is installed on a merchant's point of sale device without their knowledge. This can occur when an unsatisfied employee does this for hackers in return for monetary benefit or non-monetary gratification. Pin-pad devices utilised by many drivers throughout many industries can also lead to disaster if it has been chipped by a skimmer. Though, unless specialised knowledge is obtained, it is difficult to detect a skimming scheme. There are guidelines for detection, such as monitoring the activity of the terminals and having secondary checks done for skimming devices.

How can Data Breaches Affect the Business?

In the South African framework of commercial crime, the cyber world is facing ever-evolving threats that change daily. When we consider that, according to Kaspersky's employee wellbeing 2021 report, 46% of South African companies prefer not to disclose data breaches of employee personal information, we can make the statement that many data breaches that have occurred are not made known. In recent developments and in terms of Section 22 of Protection of Personal Information Act 4 of 2013 ("POPIA"), where there is reasonable ground to believe that the personal information of a subject has been jeopardised, the responsible party must notify the information regulator and the data subject, unless the identity of the subject cannot be established.

The Kaspersky report indicated that 20% of the organisation's that were surveyed faced incidents wherein personal data was compromised. The report advised that companies develop a clearly defined crisis plan and train employees accordingly within the best practices of the cyber security world. Their research indicated that less than half of South African organisations had already implemented security education and training to provide employees with essential information to safeguard the company against overall commercial crime risk.

The best practices that can be implemented to secure information within a business are to prompt patching and updating of software to prevent hackers from penetrating systems; Using encryption services for sensitive data; and enforcing strong credentials. This means that employees' passwords must have certain criteria to be useable. In addition to these methods using multi-factor login authentication is becoming the norm for online systems, however, this method can be

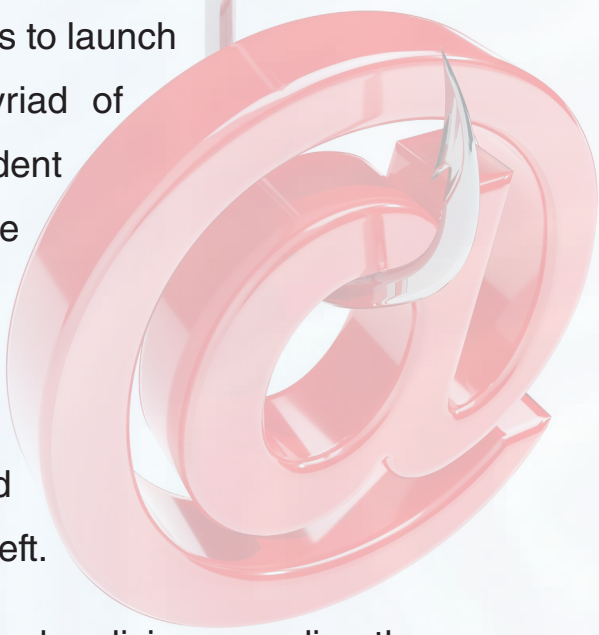
costly to small businesses. Most importantly would be to equip employees with the necessary skills they need. Even the unskilled workers can be educated with basic cyber principles as they often tend to fall prey to smishing scams. Smishing is similar to phishing emails, however in smishing the perpetrator will attempt to obtain sensitive information through the use of SMS or text messages.

One example of a data breach is the reported data breach of Dis-Chem where 3.7million client records were exposed during May 2022. This incident, as reported by My Broadband, came about during an incident involving a third-party service provider

Though Dis-chem has remained silent, as stated in their statement to tech central on the matter it can be extrapolated that the unnamed third-party service provider had a penetrative aspect to their cyber security approach. This means that larger companies can implement basic cyber security criteria on their suppliers whenever data needs to be shared. This can be especially true in the case of Dis-chem as how the data breach had occurred will not be revealed but it can be said with some certainty that it could have been prevented if all parties had exercised due diligence in terms of their cyber risk prevention by using encryption software, dual-factor authentication or by using stronger external firewalls to detect threats

The information that was collected from this incident resulted in first names and surnames, email addresses, and cellphone numbers being leaked that could possibly be used in phishing and smishing scams. Investigations into the incident are ongoing as of the writing of this newsletter and Dis-Chem has reported that the unnamed third-party operator has deployed additional safeguards, including enhancing access management protocols to act as an additional line of defense against external sources.

The s**econd example** of a data breach was reported on TimesLive in March 2022. This data breach involved the TransUnion Credit Bureau. TransUnion acknowledged that at least three million consumers are possibly affected by this data breach orchestrated by a criminal third party that gained access to the server by the misuse of a user account. This data breach had caused the suspension of the client's access where the breach had occurred and had to engage cyber security and forensic experts to launch an investigation. TransUnion confirmed that a myriad of personal information files was obtained during this incident and based on their investigation this information can be used for different purposes by criminal organisations. For example, a breach of the credit bureau Experian in 2022 exposed the personal information of as many as 24 million South Africans and after the incident had led to an increase in impersonation fraud or identity theft.



This misuse of user accounts had occurred due to weak policies regarding the user, and client, password maintenance. American Banker had reported that the data breach was possible as the user account using the password "password", thus gaining entry to the system was as simple as logging in. If controls were in place that would force users to create strong passwords many cyber security risks could be prevented. Furthermore, encrypting the information stored online with multiple separate levels of account authentication is highly advisable as businesses progress to more and more digital industries

The **third example** is from African Bank, where it was reported by Business Tech that the bank had confirmed that one of its appointed partners, Debt-IN, was targeted by cybercriminals in 2021. At the time of the report, security advisors concluded that there was no evidence that the ransomware attack had resulted in a data breach. However, Debt-IN is now aware that the personal information of certain customers, including

several African bank load customers under debt review, had been compromised. This could easily have been the entire database of African Bank clients and their personal information.

This incident had resulted in the proposal for the implementation of a robust mitigation plan by Debt-IN to contain and reduce any further adverse impact. African Bank had been collaborating with Debt-IN to address this breach and has confirmed that the relevant regulatory authorities and affected data subjects had been notified. As a precautionary measure, African Bank's fraud prevention team had taken steps to enhance the current security measures in place to protect all of their customers from a repeat data breach.

ITweb reports that African Bank had issued a statement regarding this data breach. It was made clear that this was a sophisticated attack, that bypassed the standard software that was required to keep computer data "safe". This shows that regular and robust overhauls are necessary in the IT field. Debt-IN commented that it was believed to have been targeted in April of 2021, but the cyber-attack was only picked up in September of 2021. This lapse of time allowed the criminals to obtain as many as 1.4 million personal records, exposing more and more people to cyber security risks.

Smooth-talking criminals can also cause major data breaches. Information shouldn't be disclosed over phone calls even when a trust basis has been established, it is

best practice to contact the organisation directly and then enquire upon the incident to confirm its validity. An article by My Broadband reported that criminals can keep persons online and have information available to them to completely impersonate the authority they are trying to impersonate.

This can include scams that are implemented in person with forged documents, phishing scams where user data is captured, and myriads of nefarious ways information is obtained by criminals. When this does happen, it can result in damages that not only include financial problems but also gives hackers opportunities to spread that information to other syndicates to reuse.

The **fourth and possibly most insidious example** took place within the manufacturing industry. TheatPost reports that Chinese electronics manufacturing giant Foxconn was hacked by the online group SwaggSec in 2012. Although this event took place in 2012, it is still incredibly relevant to this day as a spur to action in terms of cyber security and protection of personal information.

The cyber-attack targeted client information for Foxconn who is a prevalent supplier of Apple electronic components. However, due to partnerships with cyber technology giants such as Intel, IBM, and Microsoft there was a large amount of personal data leaked to the dark web. Foxconn remained silent about the incident but did however release a public statement confirming an overhaul of their cyber security infrastructure. But this was not the end for the melancholies that will follow in the years to come for Foxconn.

BleepingComputer reported in 2020 that another cyber-attack had occurred at the North American branch of Foxconn. During this attack ransomware was used. Clients

of the company could not access the website, but the onsite situation proved far more severe than clients not being able to access a portal. The ransomware attack happened due to an exploitation of the Foxconn system and utilised this vulnerability in their IT infrastructure to gain access to the company server. CRN reported that this was achieved by using the username for the city's manager of information systems. With some speculation it can be assumed that dual factor authentication may have been able to prevent this.

Though the first cyber-attack only stole information regarding clients and users of Foxconn, the second would prove to be most detrimental to the company. The attackers, a group referred to as DoppelPayment, requested a $34 million ransom to unencrypt the files that were inaccessible. The group was reported to state that they encrypted the whole of the North American segment of Foxconn, which is about 1200-1400 servers, and that they had obtained 75 terabytes of miscellaneous backups that may or may not contain personal information. During the attack the company lost 20-30 terabytes of data that the attackers had destroyed.

The information leaked may not seem of great consequence at first glance however there lies a deeper, far darker implication to these publications to the dark web. When this information is leaked other hacking groups immediately seize it, this information is then recycled into the next en masse attacks that are carried out through phishing or whaling (highly targeted phishing attacks that are aimed at senior executives). Through the anonymity afforded by the dark web these thieves rarely expose one another and prove almost impossible to trace unless publicly known such as Anonymous (currently involved in targeted cyber-attacks against Russia) or N4aughtysecTU.

The relevance of these examples lies in the modus operandi utilised and the vulnerability of the Information Technology environment. All businesses face similar Information Technology risk, regardless of their size and functionality. Implementing the correct

kinds of data-centric security can reduce your data breach risk to acceptable levels and protect your organisation.

Conclusion

Data breaches occur every single day, and though a person may not have been under the comb of an attack yet, it is of utmost importance to prepare for all eventualities. This becomes more and more apparent as we travel towards a more digital age. With information being kept online the opportunity for commercial crime to occur increases immensely, not only for organisations holistically, but for every single employee within them.

Bibliography

ShredNations

MyBroadBand

TimesLive

BusinessTech

TechCentral

Dischem

American Banker

Bleeping Computer

ITWeb

Threatpost

CRN