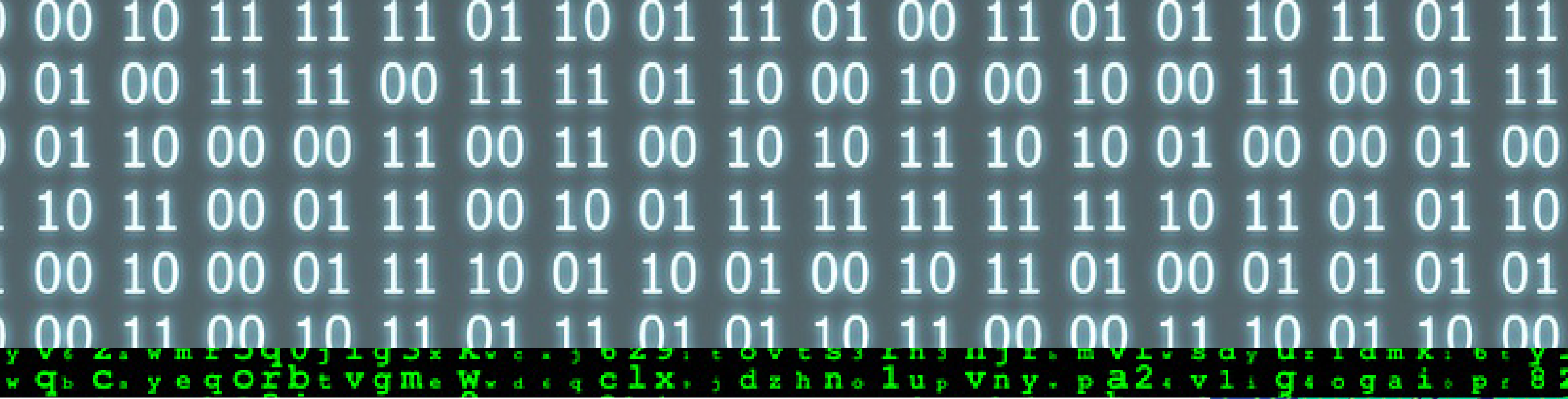

Latest cybercrime trends and the impact of commercial crime on businesses

January 2022 Newsletter
14th Edition

RMG

CELEBRATING 10
YEARS OF
SERVICE EXCELLENCE

Contents

Introduction

With the advent of digital platforms sweeping the globe businesses should recognize and be aware that risk management is paramount to operational efficiency. The future we face is a dark landscape that holds ever-evolving dangers than cannot be fully controlled. Because of the growth of technology, there is an ever increasing growth of threats. Risk management and the associated controls is nothing new for South African businesses, however in light of recent events the effects from previous threats have increased considerably. With the rise of remote work and the established need for digitisation there must still be notable considerations given to the core values of risk management. This can include re-evaluating controls and protocols and even implementing further controls to combat threats that were hitherto not a problem. When fraud has occurred, the effects can be total elimination from the market for many businesses, but with the correct procedures and protocols the impact can be lessened. This paper looks at addressing the prevention and impact of specific commercial crime spectrums and how they will apply to the day-to-day business operations.

Cyber-criminality

According to cybersecurity ventures, the world will store 200 zettabytes of data by 2025. This includes data on various infrastructures, cloud data centers and personal computing devices. Digital transformation and the commercial model have been of very high influence on the current expansion of the cyber-attack surface. A study by the UK department for digital, culture, media & sport, reported that 46% of businesses have experienced cyberattacks in the year of 2021. The most common types are malware which includes ransomware cyberattacks, spyware, or viruses which accounts for 16% of the number of attacks, and the remaining 86% is made up of phishing attempts that aid to launch a larger scale cyber-attack. We have moved into the early stages of the fourth industrial revolution that is highlighted by digital interactions and the meshing of machine and man. Our way of life is changing rapidly, hastened along by the Covid-19 pandemic. Because of the fact that many internet users are unaware of correct procedures and practices. Whereas a professional office would be well fortified with secure firewalls, routers, and access management run by IT teams, a remote worker would not always have those luxuries. Forbes has speculated that the digital transformation was advanced by up to seven years. But simultaneously criminal elements have had to change tactics to take advantage of these changes. The Internet of Things(“IoT”) describes physical objects that are embedded with sensors, processing abilities, software and other technology that connect and exchange data with other devices and systems over the internet or other communications networks.

The Internet of things is related to several supply chain vulnerabilities as supply chain cyber-attacks can be perpetrated from nation state adversaries, espionage operators, criminals, or hacktivists. Their goals are to breach contractors, systems, companies, and suppliers via the weakest links in the chain. There are many methods that hackers have employed over the decades but because of poor security practices practiced by unaware persons can be devastating to a company.

Vulcan describes malware as malicious software that includes spyware, viruses, and worms. Most common anti-viral software can protect against the more common types of damaging software, however there are certain digital menaces that are far more difficult to prevent. Ransomware, a specialised type of malware, has been a weapon of choice for hackers for over 2 decades, and is still the primary threat against businesses. And with the rise of digitisation there has been several large-scale events during 2021 that was executing using ransomware. This trend means that cyber crime groups are becoming more sophisticated in their phishing attempts by exploiting machine learning and the anonymity afforded by the dark web.

Crypto-currencies allow cyber criminals to be paid in transactions that are very difficult to trace, and thus it is slowly turning into a profit motive for some criminal entities who are replacing brick and mortar crime with digital crime. Ransomware had an estimated cost of ransomware was $20 billion in 2020, a rise from $11.5 billion in 2019 and $8 billion in 2018. That trend will continue to grow in pace as more and more businesses move over to digital platforms that will eventually require crypto-currencies to operate and manage. In order to prevent ransomware attacks is essential and will require business to up their cybersecurity awareness.

The 2020 World economic forums global risks report listed cyberattacks on critical infrastructure as a top concern. This critical infrastructure can stretch across multiple sectors that can include energy, healthcare, and transportation. According to the dragos inc. 2020 report, there is estimated that cyberthreats to industrial control systems and operational technology has increased threefold. These threats can include phishing scams, bots, ransomware, and malware and exploiting software holes. Hackers will often seek out unsecured ports and systems on industrial systems connected to the internet. For business to help facilitate risk management there must be an application of a comprehensive risk framework to address vulnerabilities to digital infrastructure.

With the emerging digital age consumers must be aware of cyber insurance, as reported by CRN. The webpage reports that this is a necessary step for some business as this will an essential in the face of network intrusions, data theft and ransomware incidents.

Social engineering is an ever-present danger as the human judgement can be swayed to give access to hackers. This term describes when hackers attempt to manipulate human psychology in order to further their goals using phishing, cat phishing, and scareware. Vulcan reports than almost 90% of the social engineering tactics employed by hackers tend towards phishing, as it is usually the first entry point of a cyber-attack.

Ransomware

Ransomware is currently the biggest threat that businesses face and as of 2021 the digital world is more at risk than ever before. The profile for who is most at risk has shifted, CRN (Computer Reseller News) reports that even the larger, well monitored technology firms that manage the data and web traffic for fortune

Notably companies such as ACER, KIA Motors and CD Projekt had suffered ransomware attacks during 2021. Though some companies can use back ups of their files to mitigate the impact of a ransomware attack, not everyone is so lucky. Hackers demanded up to $20 million for the ransom of some files.

For a small business that amount would be unreal to come forth with, but hackers tend to know how to extort a specific clientele. Privacy affairs have stated that there has been a 62% increase in ransomware on their surveys since 2019. This amount will rise as more businesses are moving towards digital platforms and hackers become more proficient in infiltrating systems and networks.

Not only does ransomware pose a significant economic and financial problem to business but it also means that operations may cease to be performed and production or sales will stop. If the ransomware cannot be overridden this could mean a major loss of revenue for a company, loss of sales or reputational risk. Facebook (now meta) and LinkedIn are also under speculation of researchers from Bank Info Security that they may aid the spread of ransomware products, essentially becoming a distribution channel for hackers to spread malicious software as software can be embedded within certain documents.

A distributed denial of services (DDoS)

A distributed denial of services attack, as described by sucuri, is a non-intrusive internet attack that can slow down or even shut down a targeted webpage by flooding the network, server or application with fake traffic. The main objective of a DDoS attack is to prevent users from accessing a specific online application or webpage. Another method that hackers employ is to send bogus requests to the target to overflow their network capacity.

Some attacks can be short burst of malicious requests on a vulnerable endpoint such as search functions. The DDoS attack can use an army of zombie devices called a botnet, that are usually comprised of internet of things devices, websites, and computers. When the botnet attacks the target, it can result in large scale financial losses and performance issues. Within this spectrum there also exists a denial of service (DoS) attack, which is very similar to the Distributed denial of service attack. They differ in the key aspect of their scale, a DoS attack would usually come from one source whereas DDoS attacks come from multiple, often spoofed, locations. This does not necessarily mean that a hacker will use only one computer, however a larger DDoS attack can span hundreds of thousands of systems.

Although DDoS attacks do not steal website visitors' information, they can be used as a way of extortion or blackmail. For example, website owners can be asked to pay a ransom for attackers to stop the DDoS attack.

There are signs that can be indications of a DDoS attack, they can include that the website is unresponsive or slow or that users have problems accessing the website. There does exist several different types of DDoS attacks that can must all be taken as highly dangerous and as an impending risk to business. Hackers use the amplification effect in order to successfully carry out DDoS attacks. This can be described using the following scenario:

One attacker can control 1000 bots, which can then be used to target one server. If one bot just needs to send 1 byte request in order to get a 100-byte response it can be observed as a x100 amplification. When the request is spoofed, the reply goes back to someone else on the internet and not to the attacker leading that the server on the attacker's side will only have to process 1byte per request.

The above-mentioned scenario would be devastating to a small business and could lead to a total shutdown in light of current economic circumstances. There are several different types of DDoS attacks that include:

- Volume based attacks that aim to overwhelm the targeted victim, which can be sub-categorized as user datagram protocol DoS attacks that will flood various ports at random, forcing the webserver to respond, which will halt or crash the server.

- Another tactic that is employed is to floor the server with spoofed Internet control message protocol packets sent from a huge set of source Ips. This will result in server overload and failure to process requests, causing the server to reboot or lead to an extensive impact on the server performance. This method will consume bandwidth to the point of server exhaustion.

Tactics can vary but hackers will usually send an email predating the attack with the necessary ransom information. This email would be nearly impossible to trace and is seen as the starting point of a DDoS campaign. There would usually be follow up emails to warn that the attack will worsen if the ransom is not paid, this ransom is usually charged in bitcoin. It is never advisable to pay the ransom since the more money malicious entities accumulate will spur their ambitions onward. It is very advisable to have consistent back ups and protection in place before a website or application is targeted for an attack.

Hacktivism occurs when hackers deploy a DDoS attack to spread a message, this motivation can be the hardest to understand as it is fueled by extremism and misinformation. DDoS attacks also occur when hackers show off their skills in order to ascertain bragging rights over an event. The usual targets of hacktivism are government, financial or large business websites. When the website shuts down due to the attack hackers can lay claim on the event through use of social media and the deep web and the dark web.

The worst motivation for a DDoS attack can furthermore be out of pure boredom and amusement. For some of humanity there exists the sadistic nature that breeds the want to see suffering. These individuals do not care about the targets of their attacks, it's the thrill of the chase that these criminals desire and they will sometimes not cease their attack after the ransom has been paid as their Internet of Things devices would usually be destroyed or abandoned in order to prolong the attack.

The impact of these attacks to business can be devastating, even as most owners won't fully understand what is happening to their website. But not all protection measures can prevent a DDoS attack. Even hosting sites are ill prepared to deal with the problem of application-based attacks. As attacks on multiple sites on the same server will eventually cause a total server shutdown, inadvertently affecting other websites. The only way to take precautions is to have a firewall in place to keep malicious traffic off of a website, to block the access of some countries (for example users from China or Russia would need a specialised login protocol) and to consistently monitor the traffic on the website. In order to fully prepare for the event of a DDoS attack, it must be clearly specified and reported in the disaster recovery plan in order to ensure successful and efficient communication, mitigation, and recovery in the event of an attack.

Hidden Threats

Not all of the emerging cyber security threats are as well known as ransomware and DDoS attacks. There are also more advanced methods that hackers employ to cause chaos and misery. Cyber reports that one such method is formjacking, this is where malicious JavaScript code is inserted into a webform, usually on a payment page. When a site visitor enters their payment card information and hits submit, that code will collect the card number as well as any other information that was entered to be submitted to another location that the attacker had chosen.

Cryptojacking is the type of cybercrime that involves the unauthorized use of people's devices by cybercriminals to mine for cryptocurrency. The motive is profit, but the aim is to stay undetected. Cryptojacking will cause serious performance issues and downtime costs as IT teams would need to track down and remove the cryptojacking code.

As the Internet of Things, which connects all devices all over the world through the internet grows, more and more areas of risk are emerging as cyber criminals are becoming more sophisticated in their approaches. A fortune business report indicated that the market scope of the Internet of Things will likely grow to approximately $1,1 trillion by 2026.

ZTNA'S

Virtual private networks (VPNs) are used to establish a secure connection between a user and the interne. Kapersky reports that a VPN is used to disguise the users IP address, essentially making the user invisible. A VPN also serves to encrypt data traffic on a website.

However as more and more businesses are making use of these tools to safeguard against ransomware and phishing schemes, VPN servers are losing their dedication and hackers are taking advantage of this. Many times, businesses will seek out cheaper alternatives and take the risk of using companies that are using out of date software and who are at risk of having a server overload due to having too many clients.

TechTarget states that some experts believe that VPN’s have struggled to adapt to the increasingly internet-dependent, cloud-based world. The solution is the Zero-Trust Network Access which many organizations are turning to as it is a more modern cloud-native security solution. The advantages of ZTNA’s are that it does not require backhauling of traffic and proves the user with a secure and safe experience. As the ZTNA is cloud native it is available across all geo locations and scales automatically based on the number of users. Whereas VPNs are appliance-based customer managed solution that establish a private and encrypted tunnel between a user and a network, ZTNA’s provides a stronger security protocol as users and devices are verified not only at the time of login but are continuously verified and validated through their user session. In addition, ZTNA’s uses the principle of least privilege that automatically defaults to the lowest level of access for all users and does not connect users or end-user devices to corporate networks.

There are many emerging and existing solution firms that are offering ZTNA’s as part of their package catalogue. It is wise for businesses that are hoping to up their security to enquire from their service provider about the use of ZTNA’s for their business. In terms of companies that do remote work this would be an essential security tool to improve a risk profile in terms of IT security.

The impact of Commercial Crime

The impact of broad-spectrum commercial crime has always been dreaded by the economic community. Lexology states that criminals are seeking to exploit any new vulnerabilities that have been introduced in recent years, digital and otherwise. With the new year approaching many businesses can look into pervasive risks and develop approaches that are proactive instead of reactive. In order to proactively prevent commercial crime from taking place management must always consider what had allowed to fraud to take place by considering the fraud triangle, which is composed of pressure to commit fraud, the rationalization that the act is ethical and then also the opportunity to commit the commercial crime act. BLSA.org states that it can include corruption, embezzlement, and money laundering, as well as the conspiracies to commit robberies and heists. Zurich.com elaborates on this and includes hacking and cyber vandalism, credit card fraud and extortion as commercial crimes. It is usually a non-violent crime that requires some modicum of specialised information to accomplish the fraudsters goals.

Currently there are new trends that are coming out that businesses need to prepare to face in the future. In order to properly govern the risks faced in the everyday business world, having tested and functional risk mitigation protocols in terms of corporate governance and due diligence is necessary to operate a functional business. There is an ever-present danger faced by corporate crime, whether internal or external, and its effects can be devastating as it can result in scandals and loss of revenue that would impact the bottom line.

Business can prevent this devastation by:

- Conducting regular and thorough risk assessments of the entire business and all of its network interactions. This will allow management to get an overview of all the risks faced in the business, this can be done internally but it is advised that specialists be used in order to have a comprehensive risk management report generated. Protocols and methods can then be put in place as controls to mitigate commercial crime from occurring

- It is advisable for businesses to identify which risks are low, medium, or high. This will allow management to focus more resources on any priority risks identified. It will also help organize the risks faced by the business in order to address all of them.

- As previously noted, the tone at the top sets the culture of a business significantly. This can help a business develop a zero tolerance of fraud and other irregular activities that do not align with the vision of the business. To successfully address these risks employers must ensure top level commitment to addressing commercial crime risks.

- Implementation of anti-fraud and corruption policies are invaluable against fraudsters, due diligence during the hiring process can sometimes identify persons who may pose a risk to the business who would not be able to comply with a business's policy. These policies can also work to raise awareness of what qualifies as commercial crime and how employees can work to take preventative measures against it.

The impact of commercial crime is lessened through financial controls that can act as early identifiers of financial statement fraud or asset misappropriation from taking place. Using the guidelines of good corporate governance, a business can mitigate several risks simply by following currently accepting business protocols.

Reputational Risk

With the rise of access to information and social media platforms the risk to the reputation of an institute has increased significantly. Investopedia defines reputational risk as a threat or danger to the good name or standing of a business or entity. Reputational risk can occur directly as the results of the company and its processes or methods, indirectly because of employees of the company. Furthermore, reputation risk can occur though peripheral parties such as joint ventures or suppliers.

It is essential to have good corporate governance practices in place alongside business transparency to be socially responsible and need to be conscious of the public perception of the business in order to avoid or minimalise reputational risk.

Reputational risk can erupt at any time with very little warning and has the potential to wipe out large amounts of market capitalisation or potential revenues. It does not always follow the top management but can also arise from the actions of errant employees.

Yahoo finance states that businesses have made large strides in recent years by addressing hiring processes and adopting confidentiality agreements with its employees. These controls can help mitigate large scale scandals arising from within the business. They recommend the following 15-step methodology to properly manage reputational risks:

1. Create a multidisciplinary team that will work together to manage reputational risks. Establish what is expected of the team, competence for performance, organisational subordination and budget.
2. Revisit the organisation's purpose. Does it still make sense in considering the ESG theme?
3. Strengthen the culture of the organisation and its entire supply chain around your purpose. Make your employees true ambassadors of organisational purpose.
4. Collect the information needed internally (in all areas of the company) to build a matrix of reputational risks.
5. Carry out the correct identification and quantification of reputational risk (experience, perception, and willingness to support).
6. Develop the prioritisation of risks using the criteria that most adhere to your organisation (e.g., probability of occurring X strength of impact).
7. Establish corporate risk mitigation strategies.
8. Understand the entire ecosystem of audiences your organisation relates to. The company needs to develop listening and relationship mechanisms with each one of them.
9. Practice the 3 fundamental Cs of communication: Coherence in speech and action, Consistency of being able to maintain communication at all points of contact, and Continuity in your value-building journey.
10. Develop narratives that are believable and above all engaging.
11. Monitor your brand awareness in traditional and social media. Make quantitative measurements and mainly qualitative analysis of your presence in the digital arena, using intelligence work and data analysis.
12. Communicate only what can be proven. A well-executed and well-communicated strategy are worth more than a thousand image bank-based posts.
13. Create an interdepartmental risk management committee that reports directly to the company's CEO to streamline decision-making and build action plans.
14. Develop metrics to understand your audiences' understanding of the company's performance. From them, analyse

expectations and perceptions.

15. Update your risk management strategy on an ongoing basis.

In addition, Ideagen has stated that there can be causes that can be identified to deal with reputational risk, as it usually can arise from poor workplace operations or conduct by an employee or a group of employees. But the problem can sometimes lie with management and higher management must always be sure to be unbiased during investigations as inadequate quality management can stem from poor operational management. This can result in poor service delivery and product quality.

How To Prevent Cybercrime

Cybermagazine reports that there are some ways that a business can protect themselves again malicious entities. Because the lower rung employees sometimes do not always know how to protect themselves. They suggest that a business must always consider the following:

ENCRYPTION

Any data with the potential to cause financial or reputational harm to an organization if it were exposed or manipulated should be encrypted. This can include using password to open files and to use additional encryption on mail servers is well advised.

BACKUP AND RECOVERY

Every company has been (or will be) hacked at one stage of their time online, and most cyber intruders go undetected for prolonged periods of time. It is therefore critical that organizations back up in ways that enable them to restore data to its unaffected pre-breach state. These back ups must be monitored consistently for any malicious or suspicious activity that may result in a security breach

CONSUMER TRANSPARENCY

All companies should not only adhere to GDPR, PoPIA and other compliance standards, but they should proactively convey it to consumers. New laws have shifted control to consumers over how their data is stored and managed — and organizations should demonstrate their commitment. Businesses who are more transparent than others in their practices may have a higher appeal to consumers as they will be able to give better assurance to their clientele.

CYBERINSURANCE

Ransomware should be covered by cyberinsurance policies — which typically reimburse for data loss damages — even if an organization is (unintentionally) negligent or imperfect in its backup practices. Insurance agencies are moving with the times and are adding Cyberinsurance packages to their portfolio such as King Price insurance and standard bank.

HIRE EXPERTS

It is critical to have people (on staff, contractors, or through vendor relationships) contractually available, at all times, with deep domain subject matter expertise in all aspects of data security — legal, technical, operational, and disaster recovery. Whether hired internally or externally there is always a benefit to having a highly skilled workforce. In addition, newer companies employ tools such as VPN's, ZTNA's and XDR systems in order to maintain security for their clients. It is not always necessary to learn the tools of the trade if experts are available for use.

It is prudent for a business to be aware of threats that reside internally. By doing surveys and consistent risk analysis businesses can gauge the amount of risk posed internally from its employees. Employees are becoming more and more adept at using technology, but sometimes it is without their knowledge that they have put themselves at risk. By raising awareness, a business is able to educate its workforce in terms of leaking information, protecting devices and the use of supported software will increase the overall cybersecurity of the entity. Intimidation or revenge against the company must also be safeguarded against. Negative employees can cause malicious harm if they gain unauthorized access or can harm the productivity of the company if repairs are required. Businesses must aim to get to know their employees in order to judge who is ethically fit to hold the mantle of responsibility.

Conclusion

Cyberthreats have been constant in their emergence, but due to the expansion of the digital world hackers and criminal elements have strengthened and refined their strikes. Businesses must be aware of the solutions offered in order to combat new threats, leading to a constant monitoring, and adapting of the IT capacity of a business. If a company does not learn to adapt to the new tactic employed by criminal elements, they will surely be overwhelmed by the force of which a cyber attack can occur. Businesses must be aware that the priority of risks are always shifting, with changes in the business environment dictating the flow of risk and public opinion. To adapt, a business must continuously re-evaluate its own actions and be able to identify where new risks have arisen. By looking at what constitutes under the banner of commercial crime businesses can identify new risks that they would not have been aware of. The new normal is setting in and businesses have started with their damage control on how to manage both existing and new risks.

Bibliography

Wikipedia
CRN
Privacy affairs
Sucuri
Cybermagazine
Onlinedegrees.edu
Investopedia
Citrix
Willistowerswatson
Sg.finance.yahoo
Forbes
Bankinfosecurity
Assets Publishing Service
CISA.gov
Acronis
Simplilearn
Techtarget
VMware
Ideagen
Cybersecurity ventures