Cyber threats in the Zimbabwean business environment
In today’s digitally driven world, information technology is a foundation for business growth and sustainability. The amount of data continues to grow exponentially, as does the rate at which organizations share data through online networks. Millions of machines such as tablets, smartphones, ATM machines, CCTVs, environmental control systems and much more are all linked together, increasing interdependencies exponentially. This increase in information, its availability and connectivity also implies losing direct control of data security.

Cyber threats are defined as the possibility of a malicious attempt to disrupt or damage computer systems. The current threats in our environment range from theft of PC’s with confidential information to ATM card cloning. Cyber criminals are aware that the market is vulnerable. Driven by a wide range of motivations, from pure financial gain, raising the profile of an ideology, to espionage or terrorism, individual hackers, activists and organized criminals are attacking government and company networks with increasing frequency and severity.

**Cyber Incidents in the Business Environment**

A minority of local businesses have made significant progress regarding their cyber security responsibilities over the past few years and most of these now boast of their impressive capabilities, controls and processes. They would not be an ‘easy target’ but they are still yet to attain an advanced level of cyber security maturity. The rest however have some catching up to do.
The majority of businesses lack discipline in some of the following areas:

- Documentation on policies and procedures in cyber security controls;
- Keeping Information and IT asset registers up to date;
- Tracking emerging threats;
- User awareness on basic security controls;
- Implementing key security patches;
- Re-configurations and system hardening of key platforms;
- Monitoring and controlling access management (particularly off-boarding of employees and contractors); and
- Back-up and recovery of critical data.

Whilst most companies would hold the current difficult economic environment responsible for failure to implement solid cyber security measures, a closer look at the areas identified above would suggest that rigor around the operating effectiveness of controls and processes that are already in place and implementation of recommended controls would boost security.

A cyber incident can be initiated either from a technical level or a non-technical level. At a technical level, the cyber incidents can be initiated at the application, database, operating system, internal network or the perimeter network technical layer/level of the IT spectrum (figure 1). At a non-technical level, cyber incidents can be initiated through social engineering techniques such as phishing scams, pretexting, baiting and so forth.

Figure 1: Technical Levels of the Information Security Spectrum

© 2020 KPMG an Zimbabwean Registered Partnership and member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
Cyber incidents are intentional attacks or unintentional breaches that can include gaining unauthorized access to digital systems to disrupt operations, corrupting data, stealing sensitive information or causing denial-of-service on business websites. Entities that use and/or retain large amounts of Personally Identifiable Information (PII) data e.g. financial institutions that process significant credit card transactions, insurance entities, healthcare organizations, and retail entities may be most vulnerable to such cyber incidents. However, PII could be stolen from entities in any industry, and the information stolen is not necessarily restricted to customer information.

The threat landscape continues to evolve. Criminals are looking to repurpose attacks used against banks to target other institutions such as insurers, e-retailers and the healthcare sector. Organisation are not by and large, dealing with scattergun attacks. Instead, they are facing a world in which their security measures are tested time and time again by highly informed, well prepared individuals and groups that target the following specific sectors:

- **Insurance**: Insurers have a wealth of data points on individuals including their health details, residential details and vehicles information. If banks hold the money, insurers hold the data. Identity fraud is therefore a significant risk. Cyber attackers will move to the point of least resistance. As banks strengthen their defences, attackers may move their focus to the insurance sector amongst others.

- **Banking**: Pressure is continuing to rise for banks to secure their digital banking channels and avoid counter fraud. The roll out of two factor authentication (authentication that requires not only a password and username but also something that the user has on them, such as a physical token) has reduced online fraud levels in the banks that are implementing it. Chip and pin has limited the ability to exploit stolen card data, but online and mobile payment (card-not-present) frauds are increasing in the market. Some shops have started demanding that customers provide extra identity verification when making such payments as a way to curb fraud.

- **Professional Services**: Lawyers, consultants, architects, engineers and accountants are a few of the professional services providers that are being increasingly targeted as the trusted route into major organisations. They often hold sensitive client data and are subject to receiving phished emails from attackers who try to lure them into sharing their client information involuntarily. This sector frequently encounters ransomware and bribery thus strong security systems and processes are highly recommended.

> “Cyber-Security is much more than a matter of IT.”
> — Stephane Nappo
- **Healthcare**: Healthcare companies such as clinics, pharmacies and hospitals are often the victims of cyber incidents as they handle the most sensitive data such as prescribed medicines, private conditions and individuals’ medical treatments. Such private data sells big on the black-market and to newspapers.

- **Retail**: Web attackers are the biggest risk for retailers operating on the e-commerce platform and offering digital services to their customers. Currently the risk is still low as majority of the payment methods are mostly semi-automated and the systems are not connected directly to the payment platforms. In the past however, criminals have accessed retail systems and created their own accounts, debited a few dollars and shopped “for free”. IT staff also sometimes forget to perform basic tasks such as reconfiguring access ports and changing default passwords to the POS terminals. Recently the point of sale devices have also been targeted as these are generating many transactions and some are directly connected to the core retail processing systems.

- **Telecommunications**: As the heart of our networked country, telecom companies attract criminal attention as a route to compromise mobile devices. They also find themselves a target of infrastructure attacks, unavailability of services, incorrect mapping of mobile wallets to user accounts and social engineering attacks on helpdesk staff.

The infographic below shows the key risks in order of relevance to some of the business sectors mentioned above:

Figure 2: Key risks in order of relevance to some of the business sectors.
The impact of Cyber Incidents on Business

A successful cyber incident can cause major damage to any business. It can affect the bottom line, as well as business' standing and consumer trust. The impact of a security breach can be broadly divided into three categories: financial, reputational and legal. These cyber incidents often result in negative consequences for the entity.

The financial cost of cyber incidents arises from theft of corporate information, theft of financial information (e.g. bank details or payment card details), theft of money, fines, disruption to trading (e.g. inability to carry out transactions online) or loss of business or contracts. Businesses that suffer cyber-breaches will also generally incur costs associated with repairing affected systems, networks and devices.

Reputational damage will erode the relationship a business has with its key stakeholders. Trust is an essential element of the business customer relationship and lack of it can lead damage relationships. The impact of this may result in loss of sales caused by the decline in demand for the business products and reduction in profits. The effect of reputational damage can even impact suppliers, or affect relationships the business has with their partners, investors and other third parties vested in the business.

Legal consequences: Organisations in sensitive sectors are typically required to actively manage the security of the data held particularly when it comes to the personal data and information. If this data is accidentally or deliberately compromised, and a business may have failed to deploy appropriate security measures, it may face fines and regulatory sanctions and these legal consequences will also result in major financial loss.
Cyber Security refers to those preventative techniques used to protect the integrity of information sent over the network, availability of programs and protection of data from attack, damage and unauthorised access. Cyber criminals around the world exploit weaknesses to steal information and money. They also target companies’ ability to deliver essential services. What is true for any organization is that cybercrime risks can be controlled.

Cyber criminals are not invincible, and while they can cause real damage to a business, one can take steps to protect themselves against them. Companies may not be able to achieve 100 percent security, but by treating cyber security as “business as usual” and balancing investment between risks and potential impacts, the organization will be well prepared to combat cybercrime.

While no two companies are the same, and there is no “one-size-fits-all” cyber security action plan, business-led protection strategies need to be embedded in governance models, operational processes, and culture. When there is a breach, your organization needs to effectively respond quickly and decisively.
Time to get serious: What Business Owners can do

The first step in improving the organization’s cyber security position is to spend some time assessing the business’ current situation. The business owners and their executive committees, must improve their awareness of the trending risks in the market, the existing controls and the gaps that need to be closed. Before investing significantly into cyber security, our experience suggests that business owners’ may want to focus on four key areas:

1. **Ownership**

   Cyber security is a business issue, not an IT issue. Business owners need to find ways to ensure that the whole business is taking ownership of cyber security and that discipline is being maintained.

   Some of the more successful business owners have elevated their Chief Security Officer to report directly to the Chief Executive Officer, creating a clear line of sight between the business and the risk. When business heads treat cyber security as an IT risk only, they risk missing opportunities and inflection points that could help fuel business growth.

   No matter what industry you’re in, data is the lifeblood of modern business. A high-quality cyber preparedness program will not only focus on keeping the data safe and secure, it will also help to increase and improve the integrity of that data to make sure that you have the right and complete data upon which to base your business decisions.

2. **Awareness**

   Since many cyberattacks stem from human susceptibility to social engineering ploys, raising awareness of cybersecurity throughout an organization is critical. In addition to intensive training programs to encourage vigilance for potentially suspicious activity, steps should be taken by senior management to foster a culture of cybersecurity, supported by dedicated champions throughout the organization.

   Improved awareness from the C-level down is key. In particular, business owners will need to focus on improving their understanding of their employees’ ecosystem, third party participants, non-affiliated agents, outsourced service providers and other non-employees with access to data, to manage their risk in a consistent manner.

   Moreover, business owners should evaluate the risk of cyber incidents across every aspect of the entity’s operations and business, including financial reporting and compliance with relevant laws and regulations through performing vulnerability assessments and penetration testing. They should also establish processes, structures and safeguards to mitigate risks.
**Capabilities**

Clearly, new and improved cyber security capabilities will be required. Business owners will also want to assess their current ‘pockets’ of cyber security excellence and work to ensure those capabilities and best practices are shared across the enterprise. Leading business owners are starting by ensuring that their existing capabilities are being properly utilised.

**In summary:** Business owners should establish if their IT environment is well equipped or well suited for its designated role or purpose in the cyber security arena.

---

**Preparedness.**

Successfully activating a response and recovery program takes practice, commitment and clear lines of responsibility. From ‘red teaming’ exercises that simulate the way an attacker behaves through to improved employee training and more frequent drills, business owners will need to carefully consider how the ensure their organisation remains prepared. To date, most have been lucky to avoid a full-scale security crisis. But this has allowed some organisations to grow complacent and let their plans and processes become stale.

Far too few organisations run regular drills or maintain updated roles and responsibilities. We believe companies that can identify and respond to emerging threats in “real-time,” by enabling uninterrupted access to prioritized data, will thrive in their business environment. These companies will stay on top of improving their preventative threat program and risk intelligence.
In conclusion

Cyber threats and cyber security are relevant to all business sectors since new technology is being used by these sectors to enable business innovation and growth. An organization framework should efficiently and appropriately address ongoing communication and direction throughout the organization. Although the local operating environment is tough, there is a lot that can be done to improve the cyber security state of any business. Business owners are encouraged to be aware of cyber threats and mitigate them by analysing their security capabilities and putting in place cyber security measures and controls starting from where they are.

This could be achieved through performing periodic network vulnerability assessments to scan, investigate, analyse, and report on any security vulnerabilities discovered on public internet-facing devices and internal networks. In addition, personnel may complete security training upon hire and a security ‘refresh training course, which focuses on IT security and access communications. These and other measures will spur the Zimbabwean businesses to success.
Chamunorwa Madziwa
Manager IT Advisory
KPMG Zimbabwe
Tel: +263 242 303700/ 302600
Email: cmadziwa@kpmg.com

Faith Maraire
Manager IT Advisory
KPMG Zimbabwe
Tel: +263 242 303700/ 302600
Email: fmaraire@kpmg.com

Disclaimer
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG an Zimbabwean Registered Partnership and member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved