Cyber risk from a chief risk officer perspective

Received (in revised form): 15th January, 2018

Jaco Grobler
is the Chief Risk Officer (CRO) for FirstRand Group, the largest financial services institution by market capitalisation in Africa. Jaco has worked extensively in the field of risk management during the past 25 years and gained extensive experience in financial services enterprise risks management. He joined the FirstRand Group in 2006 to head up the Basel II operational risk Advanced Measurement Approach (AMA) implementation across the FirstRand Group. He subsequently took up the role of Head of Financial Risk, focusing on a range of portfolio risk activities across the group. He was appointed the FirstRand Group CRO in 2010, where he is currently serving.

FirstRand Limited, 4 Merchant Place, 1 Fredman Drive, Sandton, 2196, South Africa
E-mail: jaco.grobler@firstrand.co.za

Abstract This paper provides a high-level overview of the important aspects of cyber risk management of relevance to a chief risk officer (CRO). The paper provides an overview of practical aspects to consider without going into low level technical detail. The paper also covers some of the key areas of development that must be considered in order to improve maturity of cyber risk management.

***Keywords**: cyber risk, risk management, red teaming, governance, board, encryption, incident response, information technology, vulnerabilities*

BACKGROUND

A recent study, conducted in May 2017 by ORX[1] on the future of operational risk, highlighted that most chief risk officers (CROs) and senior management have an intuitive understanding of what drives risks that are more directly associated with revenue, but are less experienced in the complexity of operational risk. The challenge with cyber risk is that it is infinitely more complex and difficult to understand than normal operational risk. It therefore creates a massive challenge for CROs to navigate through this complex subject.

These days, cyber risk is one of the most prominent risk management topics. Those who have been selling fidget spinners last year are all of a sudden cyber risk experts this year, and every consultant and vendor claims to have the 'point' solutions to address the risk effectively. Even insurance brokers are offering a spectrum of policies that claims transfer of the risks.

The purpose of this paper is to share practical experience and knowledge gained by the author spending a significant amount of time since January 2015 becoming familiar with the nature and complexity of the threat vectors. The sheer complexity and exponential growth in cyber risk makes this one of the most significant risks to focus on going forward. The more one goes into the technical aspects, the scarier it is, especially when one considers how nation state capabilities are blending with criminal activities. It is incredibly difficult for organisations to protect themselves and we are at a very early stage of the evolution of this risk type. We are bound to see significant incidents over the next few years that will overshadow what we have seen to date.

EVOLUTION OF AWARENESS

We started looking at cyber risk in a lot more detail since January 2015 and decided to change our approach and engage a boutique firm to do a very thorough red teaming test to see what is possible. As part of this approach, we had to simulate the external threat environment as

realistically as possible, including research on how the most sophisticated cybercriminal syndicates operate. Like many other firms, penetration testing was performed annually on a number of areas; however, we have never done a 'no limitations' red teaming test. The boutique firm was given the brief that there are no time or scope limitations, except that they are not allowed to bring systems down or cause any damage. The objective was to gain as much compromised access as possible and transfer funds. The exercise was coordinated from our corporate centre (head office) with very few people in the know, as we also wanted to specifically test the defences and incident response process.

Needless to say, after a couple of months the boutique firm's team achieved astounding success and we were shocked as to what they managed to achieve. We asked them to specifically focus the tail end of the engagement on 'setting off alarms'. The resulting report provided us with a huge amount of valuable information that we were able to use systematically to improve the environment. The exercise was not without controversy, including people commenting that we took a significant risk by conducting such an exercise and that they were in disagreement. The gravitas of the results and evidence, however, received so much attention, including from the board with whom we shared the results in detail, that it enabled us to propel the focus on cyber risk to a completely new level.

THE COMMON MYTHS

Before we get into the practical aspects, it is important to deal with a few of the myths around cyber risk that have been encountered along the way. The following misperceptions around cyber risk are prolific, often as a result of knowledge gaps from within organisations and from external service providers. Below are ten common myths — note there are many more that could be added to the list.

Myth 1: Core systems are secure and cannot be compromised

All systems can be compromised. Think of it as home security. There will always be a crew who is skilled enough with the right tools to break in. If your penetration test came out clean, it should be viewed with huge scepticism and probably an indication that you used the wrong parties to test it.

Myth 2: Policies and frameworks are the starting point

Cyber criminals never read your policies and frameworks, but rather look for obvious vulnerabilities to exploit. Although policies and frameworks are important to provide structure and focus, there is great risk that they can create bureaucracy and suck up valuable capacity only to satisfy auditors and regulators. Care must be taken to balance the implementation of frameworks and policies with practical and effective risk management.

Myth 3: A traditional matrix approach focusing on materiality is the best starting point

Vulnerabilities often exist in little corners where you do not expect them or where security hygiene rarely gets attention. It is often these vulnerabilities that get exploited to ultimately gain administrator access. Once admin or equivalent privileged access has been compromised, it is game over and any form of materiality matrix or crown jewel inventory becomes irrelevant. Therefore, you need to focus on every aspect and every threat vector. A traditional 80/20 approach is inadequate for cyber risk.

Myth 4: Firewall and perimeter security is the key defence

Although firewall and perimeter defence is very important, its importance often gets overstated and too much resources and funding dedicated to it. These days, there are so many other ways into the organisation. To name just a few examples: obfuscated code in e-mail, custom malware that cannot be detected, employee mobile devices, various wifi networks with inadequate security, social engineering, physical access, third party connections and so on. It is important that resources be allocated across the full spectrum of access points as there is always a way around the firewall.

Myth 5: Cyber risk is territory focused

Crime, and for that matter cyber-crime, used to be territory focused. Not anymore. Not only do the threats come from all over the globe, but we also see a significant spill-over of nation state capabilities being used by sophisticated cyber-criminal syndicates. What makes the concept of 'territories' important to cyber risk is that it is becoming increasingly difficult for law enforcement activities to take place across territories. Cyber criminals know this and exploit it. As an organisation, it makes it extremely difficult to understand who the criminal is, never mind succeeding in any form of prosecution.

Myth 6: You can utilise your existing risk management skills to deal with cyber risk

Although risk managers and auditors have an important role to play in the cyber world, they are very biased towards traditional techniques such as control frameworks, inventories, tick boxes and so on. All of which become largely inadequate to articulate a strategic response to cyber risk. The skillset required for proactive cyber risk management is much more akin to a military strategist where one looks at red and blue team capabilities. Traditional risk management capabilities would then be used to support what we refer to as blue team activities, that is, to focus on protection of the environment.

Myth 7: You can mitigate cyber risk with insurance

Bank stability is very much about reputation, a risk that can never be outsourced or transferred. As with many other vendors, cyber insurance is all of a sudden sizzling hot with numerous cyber offerings. Unfortunately, many of the cyber policies have limited coverage with large loss retentions and the value is questionable compared to traditional commercial crime policies. Cyber insurance has a long way to go from a maturity perspective, but in future it will play an important role to mitigate tail losses. Nevertheless, it will never mitigate the reputational and significant business disruption risk that cyber risk causes. Care should be taken that the board and management do not obtain a false sense of comfort by buying cyber insurance cover.

Myth 8: Data are safe because you have encryption

An audit partner said not long ago that their data are safe because it is encrypted, only to find their firm being a victim of a cyber incident shortly thereafter. Encryption is nothing other than having a key that locks the data in a digital format. People often have a false sense of comfort that their keys cannot be 'cracked'. For most high-end encryption this holds true, but what people do not understand is that the majority of encryption solutions are software based, meaning the encryption keys are either stored somewhere and probably available to be compromised, or it has already been published as compromised. In one of our penetration tests, it was possible to compromise a critical payment system. This was due to IT risk auditors that created a file containing all the users' password hashes — this file was never deleted and equated to copies of the keys being available on the file server. Hardware encryption is much safer, but it is costly and often a challenge to implement.

Myth 9: Adopting a leading cyber standard is adequate

The problem with cyber security standards is that there are so many of them out there and every regulator is trying to come up with their own definitive standard. It matters less which one you adopt, but more how you adopt it, that is, in a way that is practical and avoiding the bureaucracy trap.

Myth 10: Cyber risk should be dealt with by chief information officers (CIOs)

Although CIOs have a crucial role to play, one must think of the corporate estate as large network of pipes, processors and water flowing through this infrastructure. The parallel can be drawn that the CIOs look after the pipes. Cyber security vulnerabilities are often not caused by people in the IT community, but by employees and business leadership that are dismissive about the role

they play. In order to deal with the cyber threat effectively, it is vital to involve all role players. Cyber risk is everyone's responsibility. The CRO has a crucial role to play to ensure that all the moving parts work together.

PRACTICAL CONSIDERATIONS AND CHALLENGES

In addition to the first red teaming exercise propelling us into a whole new paradigm, we also started encountering many organisational challenges. An attempt to outline the key areas is given below.

Understanding the roles of the red team versus blue team

The concept of red teaming was originally used by the military to test force-readiness. The idea is simply that one group of security professionals (a red team) attacks the environment, and an opposing group (the blue team) defends it.

Instituting this concept in a corporate environment is, however, much more challenging. For example, it is very difficult for current staff members to fulfil the red team role as they are very biased towards their own perceptions around the effectiveness of the current control environment. Current staff also rarely think out of the box and try to find unknown vulnerabilities. Therefore, you need to create red team capabilities separate from the blue team individuals. We also found that you may have brilliant red team resources, but without transforming the blue team you will not be able to make step changes in improving the control environment. Blue team resources typically require a significant discipline and skills step up to combat the threat environment. We also found that a coordinated approach between, IT, IT risk resources, operational risk management, audit and many other disciplines are required. It cannot be emphasised enough that cyber risk is everyone's responsibility and it is vital for CROs to take ownership of ensuring all role players are actively engaged.

Although our model continues to evolve, the different skills and resources can by crudely depicted as shown in Figure 1.

Red teaming (penetration testing)

It is very important that red teaming be done as thoroughly and comprehensively as possible. Scope limitations will simply limit the value you derive from it. Every red teaming exercise we conducted

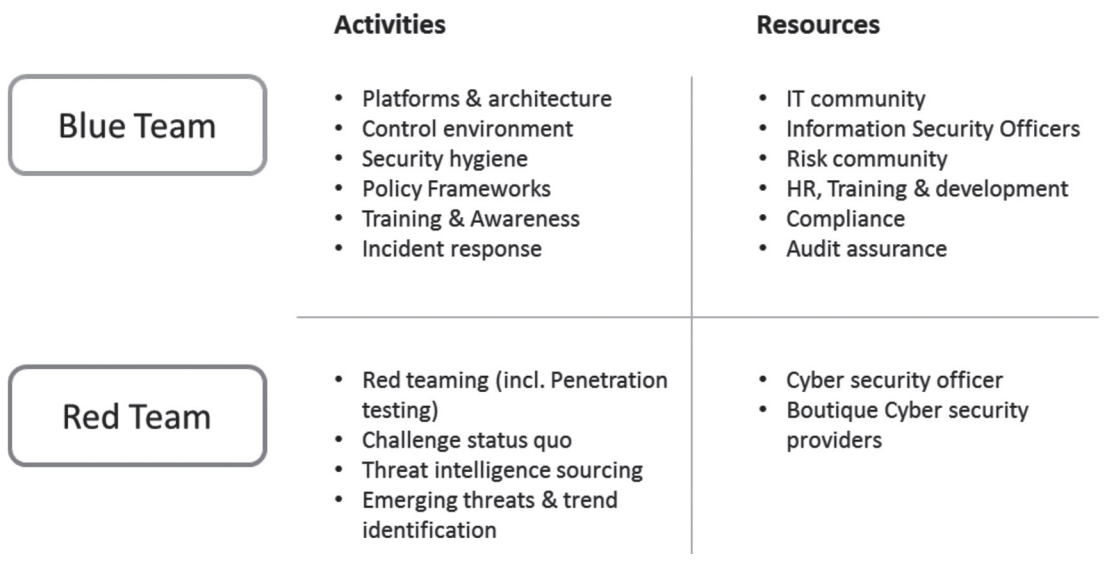

Figure 1: Blue team/red team model

enabled us to make significant step changes and close the 'low hanging fruit' gaps. Red teaming has been, by far, the most valuable part of our cyber risk effort to tangibly improve the security environment. Of crucial importance is the requirement that a very structured project plan be developed with specific interventions and work streams to close the gaps identified.

Monitoring of security hygiene

Monitoring security hygiene is not simply a house keeping matter, but is crucial to systemically manage and reduce vulnerabilities that are often exploited. Servers that are not patched or not properly configured could easily provide an 'open door' to compromise. In one of our exercises, a server of little importance (publishing non-sensitive public information) had an SQL injection vulnerability that was not patched, eventually allowing admin access to the server that could be further exploited on the network. Similarly, ransomware often also thrive on poor security hygiene. It is therefore of vital importance to institute active and ongoing security hygiene monitoring that can include, but are not limited to, tracking the following key indicators:

- Security awareness.
- Perimeter vulnerabilities.
- Server vulnerabilities.
- Device vulnerabilities.
- User access review status.
- Third party connections.
- Certificate management.
- Unsupported software.
- Expired exceptions.
- Security noise.

Technology architecture limitations

Banks have never been architected like secure nuclear power stations with security air gaps and various security protocols. Instead, banks have been architected to enable business and the flow of funds and information. As a result, everything is interconnected and it becomes very difficult to protect the so-called crown jewels, as nothing is really isolated in practice. We also found that many user authentication solutions are inadequate in their current form and have initiated a number of strategic projects in this regard, some of which are multi-year. It is very important to look at the technology and security architecture critically. Some of the important points to consider are:

- Network access control is critical at all levels.
- It is important to understand the full inventory of IT assets and devices, mainly to know which are legitimate connections and which are not.
- Limit and consolidate the various user authentication platforms to as little as possible.
- There is a good chance that your active directory solutions need to be completely re-engineered, with specific focus on how you deal with privileged accounts.
- It is very difficult to differentiate between external threats and internal threats. Once an insider's identity has been compromised, it is very difficult to detect. The use of honey pots and various intrusion detection systems are of vital importance.

Role of the CRO and risk community

Any CRO who believes that cyber risk is dealt with by their CIO or IT department without active involvement from himself/herself and other key stakeholders outside the technology space, will likely be grossly unprepared for their first major cyber risk incident.

Cyber risk is hugely complex and very different than any other risk type that we have dealt with before. The threat vectors are very different and it evolves at a very rapid pace. The complexity does not only lie in the technology space, but often also in people's behaviour and various flows of information. It is crucial that the CRO and the risk community play an active role in understanding cyber risk and proactively mitigating and preparing for incidents. At the end of the day, cyber risk is everyone's responsibility; however, the CRO plays a crucial role to ensure all the moving parts work together. It is therefore important that the CRO spends sufficient time to educate himself/herself on the nature of cyber risk and how it transmits into the organisation. It is equally import to establish a strong

team to support him/her in fulfilling his/her duties in looking after a risk that is truly systemic in nature, probably more so than any other risk type.

Role of the chief information security officer (CISO)

Most high risk organisations like financial institutions have had CISO roles for a long time. These roles have remained traditional and fairly static for some time while CISO's are often left with the challenging task to ensure adequate defence against cyber risk, but then becoming the 'fall guy' when a major incident occurs. It is not only the role of the CISO that is changing, but also more importantly the skills set required. CISO's too often embed themselves deeply in technical domains and only feel comfortable engaging with 'techies' or 'propeller heads', as some call them. The CISO of the future must be able to effectively communicate and influence at all levels in the organisation. It is absolutely crucial that he or she is able to influence not only technical resources, but also C-suite executive management to ensure cyber risk becomes part of normal risk management and business management practices. The CISO is a crucial change agent in the organisation and his or her role in education at all levels is very important to ensure a better understanding of cyber risk. In addition, the CISO also not only plays a key role to advise the CIO, but also has to act as a technology enabler, rather than be seen as the person who always says no to new initiatives owing to security concerns.

IT department priorities

While the role of the IT department in cyber risk is vast and merits a paper on its own, there are two aspects that are worth noting. First, it is often difficult for the IT department to mitigate cyber risk vulnerabilities due to cost pressures. IT cost makes out a significant part of any financial institution's cost base and there is often considerable pressure from the chief financial officer (CFO) on the IT community to reduce cost. This is where the CRO has a crucial role to play. We had an issue where a critical part of the active directory domain infrastructure had to be revamped owing to security vulnerabilities. The project got completely gridlocked due to cost constraints and role players being 'trapped' by performance targets and departmental politics. It was only after intervention from our side at C-suite level that we were able to resolve the deadlock and allocate additional funding to get the project going again. The CRO, therefore, must have sufficient insight into critical cyber risk projects in the IT department to ensure they are not deprioritised or gridlocked owing to cost constraints. Secondly, the IT department often lacks sufficient performance targets for cyber risk owing to the fact that the primary focus is placed on delivering on business requirements. What changed the dynamic for us was the significant level of education and airtime that cyber risk got at board level. Suddenly, cyber risk was such a priority topic that it could not be deprioritised by business or the IT department any more. Board directors started asking cyber questions as part of ongoing engagement with management, and it started becoming part of the ecosystem of what is important for business success.

Board training and awareness

Getting the board up to speed with the nature of cyber risk is crucial for prioritisation and momentum of cyber risk initiatives; however, also of vital importance is ensuring that the board understand the complexity of the risk and how difficult it is to mitigate and prevent incidents. We have spent multiple sessions with our board, giving them detailed insight to the nature of cyber risk and how it practically applies to the organisation. This was done via a programme we have instituted called 'Board School', where we educate the board on various risk management topics in a format less formal than an official board sitting. In one of the sessions, we spent three hours walking them through an actual red teaming exercise, illustrating to them how systems were compromised in a test and what the resultant outcome was. In another session, we spent an additional three hours with them, showing them how the cybercriminal world works, what tools and techniques are used, how transfer of funds flow and what types of activities take place on the dark web. We used numerous practical demonstrations in the sessions and made it easy to

understand for the board. Given the complexity of cyber risk, the best way to engage the board members is to get them to understand it practically.

Intelligence capabilities

Owing to the fact that cyber risk also emanates from various sources external to the organisation, it is important to build a proactive intelligence capability. This is required not only to understand new technology vulnerabilities, but also to understand what information has been compromised and how the organisation is exposed or becoming a target, for example, in dark web chat forums. Building this capability will require collaboration between specialist service providers and highly skilled employees who can interpret and translate the information for proactive risk management. Cyber risk intelligence capabilities are still at an early stage of evolution for most corporates, but will be a crucial building block for the future.

THE WAY FORWARD

Cyber risk currently features as one of the top three risks for most CROs, and at the recent Risk Minds Conference[2] it was voted the top risk for the risk community. It will remain a crucial risk and its importance will continue to grow. The level of detail we have been exposed to led us to the conclusion that most cyber risk incidents we see today are only the tip of the iceberg. The capability for much worse incidents exist and are rapidly spreading. The following trends will also contribute to an ever-increasing growth in the threat of cyber risk:

- Computing power continues to grow rapidly (Moors law), thereby increasing the capability of what is possible exponentially. Not only for the attacker, but also the number of devices as part of the internet of things (IoT) phenomenon that are exposing the organisation.
- The rise of Fintech not only creates many strategic and business challenges for banks, but also introduce significant cyber risk owing to the use of undesirable practices such as screen scraping of login credentials.
- Cyber weapons are being commoditised at an alarming rate and are now more freely available than ever before. This trend will continue.
- Nation state cyber-attack capabilities are often being used by cyber criminals. Perhaps because these actors are often used to perform rogue activities on behalf of nation states.
- Insiders are always a source of significant risk exposure owing to the trusted access and knowledge they have. The rise of populism and the 'Snowden effect' makes it ever more difficult to deal with threats from within the organisation.
- Cyber-criminal activity as a service is readily available on the dark web and the number of service providers are growing. Therefore, you do not need to have any level of technical expertise to engage in cyber-criminal activities now. You can merely source and sub-contract what you require.

It is, however, not all bad news. We see significant progress and collaboration among industry bodies and law enforcement. Everyone is taking the threat seriously and we have no doubt that for the risk professional, cyber risk will be one of the most interesting domains, providing exciting career opportunities.

References

1 ORX/McKinsey (2017) 'Future of operational risk', 15th May.
2 Risk Minds Conference, Amsterdam, 4–8th December, 2017.