BIZCOMMUNITY

SA banks and the new G7 cybersecurity guidelines

By Sharon Snell

7 Nov 2016

In a collaborative effort to improve cybersecurity in the financial sector, the G7 finance ministers and central bank governors have endorsed the G7 Fundamental Elements of Cybersecurity for the Financial Sector.

The guidelines are non-binding and represent best practice in cybersecurity. They are applicable to both public and private financial sector entities and have been designed to accommodate the size of each entity and the nature of the cyber risks it faces.

© Marie Nimrichterova 123rf.com

Banks in South Africa

There are no specific laws or guidelines for cybersecurity governance of banks in South Africa. The newly released King IV Corporate Governance Report provides limited guidance for managing cybersecurity risks. The Cybercrime and Cybersecurity Bill, which is expected to be introduced in parliament later this year, also does not provide governance guidelines. In the absence of specific guidelines, the country's banking sector should consider aligning with the G7 guidelines.

Cost of cyber-attacks

The frequency and severity of cyber-attacks have grown, costing consumers $158bn in 2015, according to Cybersecurity Ventures research. They predict that global cybersecurity costs will grow to $6trn annually by 2021 and these will include:

- Damages and destruction of data
- Fraud, embezzlement, theft of money, intellectual property and personal and financial data
- Business interruption and costs associated with loss in productivity, restoring and deleting hacked data systems and post-attack disruptions

So serious is the threat that the US president Barack Obama declared a national state of emergency to deal with cybercrime, which is to national borders and can originate anywhere in the world.

The spectacular cyber-heist on the Bangladesh Bank in 2016 resulted in theft of $81m, and was the largest hack on a bank to date. The forensic investigation revealed that malware was installed within the bank's system some time prior to the hack. The malware gathered information on all the bank’s operational procedures, allowing the theft.

Eight key elements in the new guidelines

1. Cybersecurity strategy and framework
   Financial sector entities must establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks, in line with international, national, and industry standards and guidelines.Such a strategy should specify how to identify, manage, and reduce cyber risks effectively in an integrated and comprehensive manner. These should be tailored to the nature, size, complexity, risk profile, and culture of the business.
2. Governance
   The roles and responsibilities of personnel implementing, managing, and overseeing the framework should be clearly defined to ensure accountability; and provide adequate resources, appropriate authority, and access to the governing authority.Boards or oversight bodies of both private entities and government should establish the tolerance of their organisation to cyber-attack, and oversee the design, implementation, and effectiveness of related cybersecurity programmes.
3. Risk and control assessment
   Ideally, as part of an enterprise-risk management programme, entities should evaluate the inherent cyber risk presented by the people, processes, technology, and underlying data that support each identified function, activity, product, and service. In addition to evaluating its own cyber risks, the risk the organisation presents to others and the financial sector as a whole should also be considered. Government entities should also investigate their points of weakness and put the necessary protective measures in place.
4. Monitoring
   Systematic monitoring processes need to be established to rapidly detect cyber incidents and these should be tested regularly through audits and exercises. Depending on the nature of an entity and its cyber-risk profile and control environment, the guidelines advise that the testing process be carried out by independent auditors.
5. Response
   As part of their risk and control assessments, entities should implement incident response policies. Among other things, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders. Exercising protocols within and among entities and public authorities contributes to more effective responses. Therefore cyberattacks should be publically reported to create an awareness of the nature of the threat within the industry, even though many enterprises fear that doing so could create distrust among their clients.
6. Recovery
   Resume operations responsibly, while allowing for continued remediation, including by (a)eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.Once operational stability and integrity are assured, prompt and effective recovery of operations should be based on prioritising critical economic and other functions and in accordance with objectives set by the relevant public authorities.
7. Information sharing
   Sharing reliable, actionable cybersecurity information with internal and external stakeholders and beyond on threats, vulnerabilities, incidents, and responses will enhance defences, limit damage, increase situational awareness, and broaden learning. Threat indicators or details on how vulnerabilities were exploited, allows entities to remain up-to-date in their defences and learn about emerging methods used by attackers. It deepens the collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability. Given its importance, entities and public authorities should identify and address impediments to information sharing.
8. Continuous learning
   Cyber threats and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. The composition of the financial sector also changes over time, as new types of entities, products, and services emerge,

and third-party service providers are increasingly relied upon. Entity-specific, as well as sector-wide, cybersecurity strategies and frameworks need periodic review and update to adapt to changes in the threat and control environment, enhance user awareness, and to effectively deploy resources.Other sectors, such as energy and telecommunications, present external dependencies; therefore, entities and public authorities should consider developments in these sectors as part of any review process.

ABOUT SHARON SNELL

Sharon Snell holds a masters degree in law, and she is the Chief Executive Officer of the National Museum located in Bloemfontein.

- Green reporting will expose risky companies - 5 Jul 2017
- However you word it, Uber is a taxi company... UK ruling says - 8 Dec 2016
- SA banks and the new G7 cybersecurity guidelines - 7 Nov 2016
- Counting the cost of #FeesMustFall and other protests - 17 Oct 2016
- US insurer ordered to defend prescription drug lawsuit - 26 Sep 2016

View my profile and articles...