INFORMATION NOTE 008 - CYBER SECURITY RISK CONSIDERATIONS FOR ALL ACTUARIES

Classification

This document is classified as an Information Note.

Abstract

Today's actuaries have instantaneous access to information online, but always-on connectivity also carries the risk of falling victim to cybercrime, the consequences of which can be career limiting. Cybersecurity risks have therefore become a principal focus area for most institutions.

Purpose

This Information Note will primarily focus on managing cybersecurity risk (or cyber risk) as opposed to pricing cyber risk in an actuarial capacity. Thinking about potential implications will encourage actuaries to seek appropriate guidance when making cyber risk-based decisions. Many of the points discussed here will also be applicable to the day-to-day lives of actuaries in their personal capacities. By gaining knowledge, actuaries will be in a better position to assess cyber risk when pricing, even though the methodology involved is beyond the scope of this Information Note.

Legislation or authority

This Information Note is produced under the auspices of the Actuarial Society of South Africa (ASSA) System and Technology Committee.

Application

ASSA members providing actuarial support in data and cyber risk fields.

Author(s)

Actuarial Society of South Africa System and Technology Committee.

Status

Version 1.0 Effective from September 2021

1. Introduction

Cyber risk is risk that exists within the digital space. It includes risks that could lead to regulatory non-compliance, financial or reputational loss, or damage or disruption to business resulting from a direct failure of information or digital systems.

The context of this Information Note is the risk environment related to unauthorised access to data by criminal elements seeking to cause damage or loss within the digital space (The IRM, n.d.) – precisely the sort of cybersecurity risks areas in which actuaries could be involved.

From a pricing perspective, many additional risk factors would need to be considered, but as noted, the cyber risk pricing sphere will not be discussed here.

2. Current Legislative Landscape

Actuaries should be well versed - or at the very least, aware - of legislation in their respective actuarial fields as this forms a fundamental part of their professional knowledge and is covered by the actuarial code of conduct for ASSA. (ASSA, 2021)

Despite this, the modern business environment is fraught with cyber risk and general actuarial professionals may not necessarily be aware of all relevant legislative provisions. Best practice would suggest an awareness of all applicable cyber legislation, or the seeking of advice from other professionals who specialise in the cyber field where this risk could potentially impact the actuary's professional duties and responsibilities.

There are two main categories of cyber legislation, namely:
- Data protection and privacy; and
- Cyber Crimes (AmTrust, n.d.)

The first of these is more applicable to actuaries; however, a criminal looking to exploit negligence on the part of an actuary would fall under the second category - and the actuary could still be held liable. We will therefore give a few examples of data privacy laws and leave Cyber Crimes legislation to further reading as it falls outside the intended remit of this Information Note. We will however outline some basic guidelines that could lessen the chances of an actuary becoming a victim of cybercrime.

Before conducting a review of the legislation, we must first define what data protection and privacy entails in a broad definition:

"Data protection means keeping data safe from unauthorised access. Data privacy means empowering your users to make their own decisions about who can process their data and for what purpose." (GDPR EU, n.d.)

2.1. Data Privacy and Protection Legislation

The list of legislation pertaining to data privacy and protection is extremely long; however, here are some of the most prominent statutes that are likely to apply to the work of contemporary actuaries.

2.1.1. General Data Protection Regulation ("GDPR")

The GDPR legislation was drafted in the European Union and covers all EU citizens and the actions of any person or organisation aiming to collect data on, and target marketing at, any person within the EU. The provisions of the GDPR continue to apply to the UK, even post-Brexit. GDPR applies mainly to personal data (defined as any information relating to a directly or indirectly identifiable individual).

The GDPR in essence imposes fines on any organisation or person breaking the rules laid down by the legislation within an EU context.

The GDPR is based on seven key principles:
- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability

(GDPR, n.d.)

Over and above these principles, the GDPR also requires consent or a valid reason to process personal information as outlined in Article 6 of the GDPR legislation; it also defines roles within the data space. The key takeaway is that any actuary working with data would be seen as processing data in this context.

This piece of legislation is extremely involved, and actuaries will need to understand the obligations it imposes on them by reviewing the legislation and determining where it would be relevant to their actions in their professional capacity.

2.1.2. Protection of Personal Information Act ("POPIA")

As a local statute, POPIA is more relevant in the South African context and again pertains to personal information and provides various guidelines on how it should be treated.

The one thing to note is that breaches of the Act can lead to either a fine or imprisonment. This Act does not however outline a scale of penalties – rather, they will be determined on a case-by-case basis. (POPIA, 2021) This makes it extremely hard to conduct a proper risk assessment.

The actuary is generally not accountable for the data within the organisation; however, the one critical provision is that data breaches should be reported, and that significant care should be taken to make sure that data is not exposed to unauthorised parties.

This becomes a near-impossible task even with best practices, so actuaries should attempt to make sure that where access is given to data it has been properly anonymised or has been granted by a process where another internal stakeholder must also approve the access. An act as simple as sharing a cloud link can easily cause a breach even when not acting with negligence. As far as possible, company guidelines and policies therefore must be followed to prevent exposure to POPIA for actuaries. (Michalsons , n.d.).

2.2. Financial Regulations

Financial regulation might seem out of place in this paper; however, with the previous section as a pretext, it is clear that financial regulation can start to affect actuaries.

The data-sensitive nature of financial regulations is the main driver. Some of these regulations are outlined below.

2.2.1. IFRS 17

IFRS 17 is a new accounting standard that will be effective from 1 January 2023 in the insurance sector. This standard is extremely data-intensive and could potentially require some forms of personal data to be used in the valuations. (Deloitte, n.d.)

Policies must be categorised as onerous and non-onerous which means a history of the policies would have to be kept. The challenge here for actuaries is that suddenly we use data in a day-to-day operational environment, and should a breach occur in the actuarial space, tough questions would have to be answered. (EFRAG, n.d.)

Here again other professionals would be better suited to maintain a secure environment, but as will become apparent later in this Information Note, the human element (i.e., the actuary) can fall victim to some form of cybercrime resulting in a falling foul of legislation.

2.2.2. South African Prudential Standards

South Africa has prudential solvency requirements that are remarkably similar to the Solvency II standards in the European Union. These standards are not as data-intensive unless an internal model is used that relies heavily on data.

Again, depending on data access and personal information, significant risks exist for actuaries within protection of data legislation.

2.3. Limitations

As we all work in different jurisdictions and different settings, the line between the personal and the professional has become increasingly blurred. This Information Note therefore aims to create general awareness and scope a general context for the actuary to mitigate cyber risk. This is by no means a document that can be used to make critical cyber security decisions without extensive additional reading, professional guidance, or research.

The onus is on the actuary to supplement the information within this document with the sound judgement, legislation, and best practices most suited to their circumstances. Therefore, this Information Note may not be able to adequately address every conceivable situation.

The best practice would be to consult specialists in the cyber field, legislation, and company policies to come to an informed decision on what the best procedures are for the individual in any given context. Legislation is ever-changing, and nothing in this Information Note should not be construed as legal advice or as the source of the only relevant interpretation of legislation within the cyber and professional spaces.

3. Cybersecurity

In a recently published IAA paper, cybersecurity was defined as the practice of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. Cybersecurity is tasked with protecting three aspects of digital information and systems: confidentiality, availability and integrity.

Examples of specialty areas of cybersecurity include:

- Network security: Protecting the networks that host and transmit information;

- Client/device security: Protecting devices that are used to access information;
- Cloud security: Protecting cloud-hosted infrastructure and applications;
- Physical security: Protecting the physical premises that host information;
- Application security: Protecting the software applications that access the information; and
- Database security: Protecting the databases that store information.

A cyberattack (or breach of cybersecurity) is the actual act perpetrated by cybercriminals. Cyberattacks can be categorised into four types:

- Internal malicious: Where an employee of an organisation intentionally commits the attack;
- Internal unintentional: Where an employee unknowingly commits the cyber breach. This risk can be mitigated by training users;
- External malicious: Where someone outside the organisation intentionally attacks an organisation's IT infrastructure to gain access to proprietary information or for other reasons. These incidents may make it into the news; and
- External unintentional: Where someone outside the organisation unknowingly commits the cyber breach. This can be mitigated by ensuring robust protocols and training of the public.

4. Types of Cybersecurity Risk

Below are a few examples of how cybersecurity can be breached, taken from the recently published IAA paper:

- Account takeover: Online accounts can be taken over or 'hijacked' by hackers, with 'identity theft' being a common approach;
- Credential stuffing: This occurs because people reuse the same username and password across multiple websites, apps and services. If a network breach happens, the hackers steal usernames and passwords use the same username-and-password combination to access users' accounts;
- Brute force/dictionary attacks: 'Password123' is still the most popular password in the world. People tend to use simple and easy-to-guess passwords. Attackers are, therefore, able to guess users' passwords with a surprisingly high degree of success;
- Phishing/SMShing: This is a technique, which uses social engineering, to fool users into handing over their login credentials to the criminals. This is done in phishing via email and SMShing via SMS message;
- Man-in-the-middle malware: This is a high-tech technique where the bank customer's computer is infected with a virus (malware) after they visit a malicious website or open a malicious email;
- SQL injection: A bot tries to inject SQL code into a web form on a bank's website. This process is automated since there are a large number of potential weaknesses that need to be tested;
- DDOS (distributed denial of service): This is when a bot makes a very large number of requests of a bank's servers with the hope of overwhelming the servers and causing them to go offline. This will result in the bank's customers being unable to transact;
- Vulnerability exploits: Old and outdated computer systems that have not been patched or updated to address known security vulnerabilities;
- Physical breach: This is a scenario where the attackers are able to get into the bank's data centres or corporate offices and gain access to a terminal;
- Third-party breach: The hackers might gain access to the bank's networks by breaching the bank's partners – e.g. contractors developing the bank's systems or open-source projects; and
- Insider threats: When a trusted employee engages in criminal activity against the company.

5. Areas Where Actuaries Can Be Involved

Regulatory: Actuaries could become involved in shaping legislative changes and those regulations that affect their practise areas.

Risk reduction and mitigation: Actuaries, due to their expertise in enterprise risk management, can perform the role of Chief Risk Officer, or another risk management role. In this role, an actuary is responsible for the identification, reduction and mitigation of risks, including cybersecurity risks to the company.

Cybersecurity data analytics: Machine-learning models can be trained to detect these cyber threats and utilised for their automatic detection and mitigation. This is a role that actuaries can play in the cybersecurity space given their analytical expertise.

Cryptography: Cryptography is a field of study that deals with the encryption of information. . Actuaries can play an important role in the world of cryptography, using their in-depth understanding of mathematics and modelling.

The above list was taken from the recently published IAA paper.

6. Principles That Organisations Can Apply to Manage Cybersecurity Risk

- Have an organisational policy and strategy in place and ensure risk is within appetite;
- Conduct frequent training and relevant awareness programmes, including crisis plans;
- Perform frequent threat and vulnerability assessments and control monitoring;
- Implement data management, protection and encryption schemes;
- Install and/or update cyber security, risk prevention and encryption software on all devices;
- Implement appropriate access, password management solutions and segregation of duties;
- Develop robust incident management processes and procedures;
- Assign key responsible and accountable individuals to manage cyber risk;
- Report key performance indicators to the Board; and
- Prepare senior management on how to respond to organisation-wide incidents and have cyber liability insurance in place.

7. Abbreviations

ASSA: Actuarial Society of South Africa
GDPR: General Data Protection Regulation
EU: European Union
IAA: International Actuarial Association
IFRS: International Financial Reporting Standards
POPIA: Protection of Personal Information Act

8. Further Work

Cyber risk is an ever-evolving field and will need to be continually monitored in order to keep up to date with the latest trends.

Pricing of cyber risk is an interesting if technical field and something we could explore in future. Currently, this would fall more under the General Insurance category but is something we would explore in future.

Another area to be explored in future is guidelines on how an actuary can navigate a modern world rife with cyber risk without exposure to such risk in the absence of some form of best practise to fall back onto, should it ever be required.

Blockchain and cryptocurrency are also emerging areas of risk that deserve attention.

9. References & Works Cited

AmTrust, n.d. AM Trust Financial. Available at: https://amtrustfinancial.com/blog/small-business/cybersecurity-vs-data-privacy

ASSA, 2021. Code Of Conduct 2015. https://www.actuarialsociety.org.za/download/professional-conduct/?wpdmdl=1576%27;return%20false;%22%3EDownload%3C/a%3E%20%20%20%20%20%20%20%20%3C/div%3E%20%20%20%20%20%20%20%20%3Cdiv%20class=%22media-body%22%3E%20%20%20%20%20%20%20%20%20%20%20%3Ch3%20

GDPR EU, n.d. GDPR. GDPR, n.d. Article 5-2 GDPR. https://gdpr.eu/data-privacy/

Recently published IAA paper (June 2021). https://www.actuaries.org/IAA/Documents/Publications/Papers/Opportunities_Applying_Actuarial_Techniques_Banking.pdf