Chapter 6
Cybersecurity

Cybersecurity

Key points

- Cybersecurity is a serious and widespread challenge for financial services, with significant impact on both consumers and businesses.
- Commonwealth member countries must invest in both technology and training.
- A disciplined cybersecurity approach will look at systems, people and processes, and the 2018 Commonwealth Cyber Declaration enshrines these key principles.[1]

6.1 Introduction

Cybersecurity remains one of the major challenges for financial institutions around the world. A lack of digital literacy and underinvestment in technology systems has resulted in a weak cyber infrastructure that has seen not only hundreds of millions of pounds stolen, but also billions of people's personal information (including irreplaceable biometric data files).

The Commonwealth Secretariat issued a Cyber Declaration at its Heads of Government meeting in April 2018, committing to a series of principles and actions around cybersecurity. The major thematic components of the Declaration were developing '[a] cyberspace that supports economic and social development and rights online ... [b]uild[ing] the foundations of an effective national cybersecurity response ... [and p]romot[ing] stability in cyberspace through international co-operation'.[2]

To address issues of cybersecurity, governments must:

- improve the digital capacities of all government executives and professionals;
- invest in better cyber solutions;
- regulate to protect consumer and business data and assets, without unduly restricting access;
- adopt harmonised, interoperable, global standards; and
- extend the rights of citizens offline into their online experiences.

6.2 Context

More than 60 per cent of cyber breaches result from human action, whether it be accidental or malicious. Cybersecurity weakness is often a consequence of human error.

Numerous Commonwealth countries have experienced large-scale and significant cyber incidents in recent years, and the trend will accelerate as independent (criminal) cyber thieves and state-sponsored cyberterrorism and espionage become more sophisticated. Cyber attackers are taking advantage of advances in artificial intelligence (AI) and big data/big data analytics that rapidly outstrip the capabilities of national systems. Highly sophisticated personality profiling and even 'humint'

> More than 60 per cent of cyber breaches result from human action, whether it be accidental or malicious. Cybersecurity weakness is often a consequence of human error.

(i.e., human intelligence) on key targets have increased the level of risk.

Efforts to mitigate cyber risk have at times done more harm than good. For example, fingerprint and facial recognition are biometric forms of data that are often perceived to be 'stronger' than others—and yet they introduce new risks. If someone steals our password, we can change that password; if someone steals our fingerprint file, we can do nothing to change our fingertips—and a hacker can use a 3D printer to recreate that print in minutes.

6.2.1 Device- and System-level Security

Some hackers take advantage of poor discipline in relation to updating operating systems or implementing firewalls. As low-cost internet devices proliferate, often with minimal or no cybersecurity, new vulnerabilities are entering the system. (According to cyber expert Howard Shrobe of MIT, many devices still use old, unpatched versions of Linux software—meaning that hackers can exploit a series of well-known issues.) At the national level, some countries have failed to invest in upgrading computer systems within the financial services sector itself, which exposes core banking functions to serious risk and has resulted in attacks in which tens of millions of pounds are stolen in a matter of minutes.

6.2.2 Access Control

When we speak of 'access control', we are talking about controlling access by using aspects of identity. The three components of access control are validation, verification and authentication.

- **Validation** means making sure that the identity data given is real data, for example, that the National Insurance (NI) number given for an individual is not that of someone who is dead, or that an account number refers to a live account and not a closed account.
- **Verification** involves making sure that the information given is genuinely associated with a specific person, for example, that the date of birth and home address given actually belong to that person, or that the account they are trying to access is an account in that name or to which that person has legal access.
- **Authentication** is the process whereby we determine that a particular individual is who they claim to be.

All three of these components are required for a secure identity scheme. Traditional access control—the type of security we commonly use to access our accounts or computer systems—uses

elements such as a user name, a password and/or a personal identification number (PIN) code. In the modern world, if people were to use a different password for every account or system that they needed to access, they would typically need to remember 140–160 distinct passwords—and so the likelihood is that most individuals will reuse passwords, set weak passwords or in other ways compromise their online security.

6.3 Description

We can think through the elements of effective cybersecurity in terms of three key factors: systems, people and processes.

6.3.1 Systems

On a systems level, cybersecurity architects will examine the various components of a computer system and determine how each can be 'hardened' against breach or misuse. For example, some breaches have seen large companies such as Facebook storing passwords in plain text form. Encryption, which uses maths to make plain text or data unreadable, is one part of a robust cybersecurity scheme and central banks can, for example, require that the commercial, retail and institutional banks under their oversight follow industry best practices. This will include encrypting data at rest and data in flight, including passwords and PIN codes, and annual certification by third-party firms, such as EY (formerly Ernst & Young), Deloitte, Accenture, IBM, TCS or other consultancies.

Good cybersecurity hygiene will also include the following elements.

- **Vulnerability assessment** An inventory of the core financial system should be conducted on at least an annual basis, to identify vulnerabilities and recommend remedies.

- **Monitoring and intrusion detection** Systems focused on both technology and processes must be put in place to trigger early alert of any cyber incident and swift response. For example, AI systems should be the first line of defence and they should begin to manage risk as soon as an incident is detected. This might involve throttling or controlling the pace of transactions, or requiring additional approvals before significant transactions or transaction patterns can be processed. At all times, day and night, a responsible individual must be on hand to make decisions during a cyber incident. More sophisticated systems can alert a bank employee if they are looking at types of data, or at patterns of data, that could be worthy of investigation.

- **Penetration testing** 'White hat' hackers should be engaged, ideally monthly, to test government and private sector systems. They should use both electronic tools and software, as well as 'social engineering', to identifyweaknesses and suggest remedies.

6.3.2 People

Increased cybersecurity at a systems level must be partnered with efforts to raise levels of digital literacy among central bank officials, as well as banking professionals in the private sector. Cyber risk can be mitigated if professionals are more aware, better disciplined and change their behaviours when it comes to handling data. Given that human error is often at the root of breaches of cybersecurity, ongoing training is essential to instil good cyber hygiene across all institutions.

6.3.3 Processes

Tied to the culture shift needed among people is the design and implementation of better cyber processes that align behaviours with outcomes. This includes:

- identifying and eliminating redundant processes;
- regularly repeating activities to identify and remedy vulnerabilities;
- steps to identify and manage areas vulnerable to human error; and
- establishing formal mechanisms to identify new cyber threats and new cybersecurity technologies, and to rapidly respond to each.

> Given that human error is often at the root of breaches of cybersecurity, ongoing training is essential to instil good cyber hygiene across all institutions.

6.4 Key Considerations for Future Development

Commonwealth countries need to invest significantly more in cybersecurity, given how vulnerable to attack the financial services sector is, not only within the Commonwealth but also globally. Cybersecurity is an area of technology in which we commonly underinvest, paying attention to it only after the fact of an incident. With financial services systems so highly interconnected, the risk that a breach in a country outside the Commonwealth would nonetheless impact on member countries is high.

We need approaches that are more sophisticated. Strong cybersecurity can unlock meaningful opportunities for countries, including financial inclusion and economic development, and it is inextricably linked with, for example, issues of digital identity. For example, verification and authentication are critical to both securing systems and facilitating financial inclusion via identity inclusion.

One barrier to the broader implementation of improved cybersecurity is the absence of standards in a number of mission-critical areas. A consultative, multistakeholder process will help us to shape, implement and uphold such standards.

Likewise, given that more than 60 per cent of cybersecurity breaches result from human error or action, investing in digital literacy will help consumers and institutions, both private and public, to mitigate the risks.

Endnotes

1 The Commonwealth (2018). *Commonwealth Cyber Declaration*. Retrieved from https://thecommonwealth.org/commonwealth-cyber-declaration

2 *Ibid.*