The National Cybersecurity Committee

Protecting the citizens and the critical infrastructure of Mauritius

Dr. Didier Samfat
Chairman NCC

2024

OVERVIEW

Content

CYBERSPACE IS HOSTILE - THE SAD REALITY

Unveiling Cybercriminals at Work

Technical virtuosos
Innovative

Relentless
Adaptative

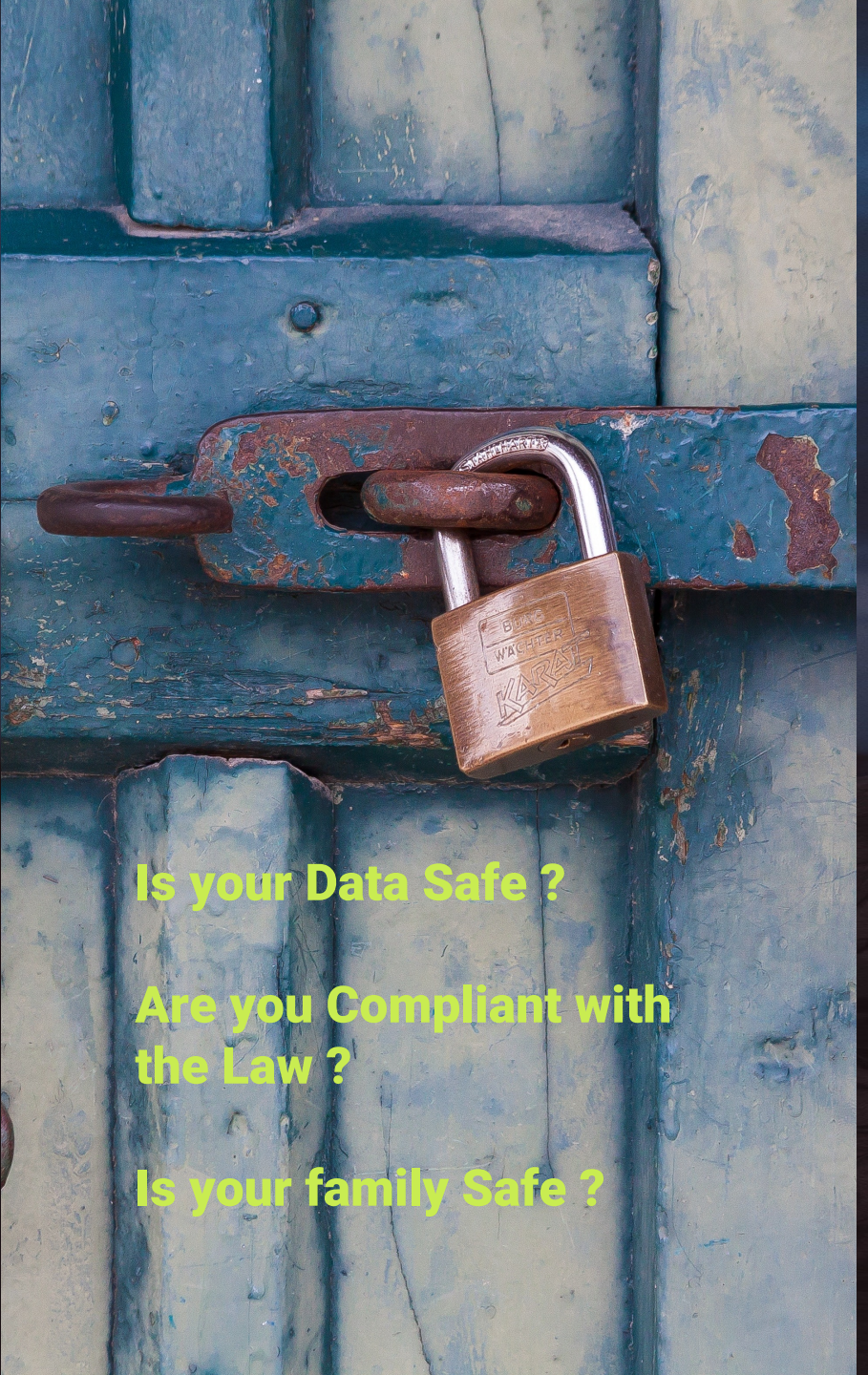
Business Email Compromise, **BEC** scams made 19,369 victims with **$1.8 Billion** – *FBI*

300,000 Malware are newly created **every day** - *AAG*

277 Days to identify and contain a **data breach** - *IBM*

Every **39 seconds** there is a hacker attack - *Security Magazine*

4.1 Million websites contain **malware** at any one time – *Astra*



Is your Data Safe ?

Are you Compliant with the Law ?

Is your family Safe ?

UNMASKING THE IMPACT

The High Stakes of Cybercrime

$400 billion of losses due to Cyberattacks yearly around the globe in 2019
- Forbes

Expenditure on information security and risk management will reach $188.336 Billion in 2023
- Gartner

Ransomware increased by 485% in 2020, with average ransom demand of $178,254
- Group-IB

Global Cybercrime costs $8 trillion in 2023 and up to $10.5 Trillion by 2025
- Cybersecurity Ventures

80% of reported security incidents were phishing attacks in 2020
- Verizon

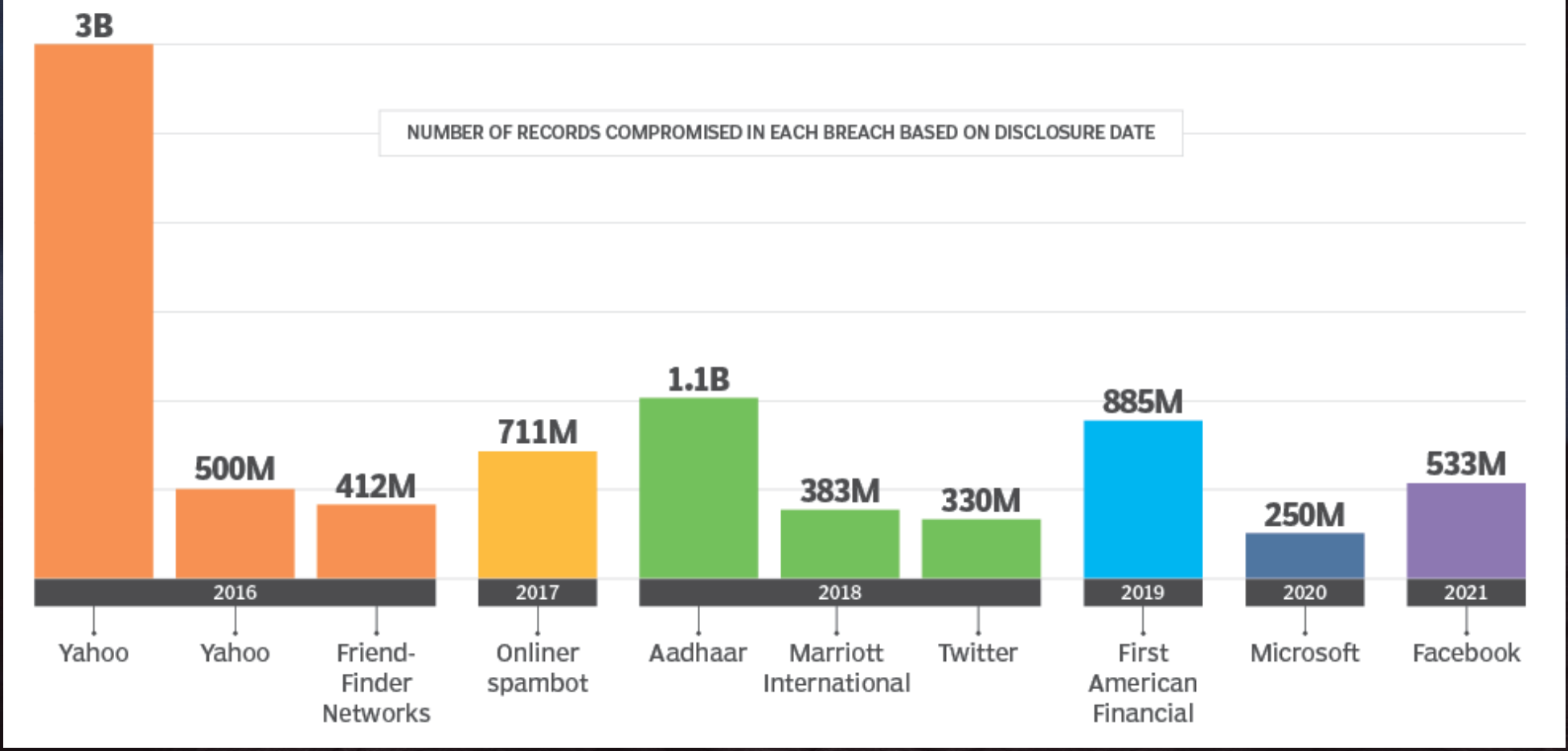
847,376 complaints in 2021 with $6.9 Billion losses
- FBI

45% of global organizations will be impacted by a supply chain attack by 2025
- Gartner

Average total cost of Data breach in 2020 was $3.86 Million
- IBM Security

TOP 10

Biggest data breaches in history



" Protectors must be right all the time, Hackers just once !!! "

- Source: TechTarget

DEBUNKING COMMON CYBERSECURITY MYTHS

SMB Reality: The Urgency to Defend

MYTHS

60% of SMBs aren't protected because they think they're "too small to be a target"
- Digital.com

"We don't need to update our software regularly"

"Cybersecurity is solely the IT department's responsibility"

"Antivirus software is enough"

"Threats only come from outside sources"

"Our employees won't fall for phishing scams"

"My data isn't important, it's not a big deal if I am hacked"

"We don't need a firewall, all our apps are cloud based"

FACTS

61% of SMBs reported a cyberattack
– Forbes

37% of SMBs hit by **ransomware** had fewer than 100 employees - *StrongDM*

SMBs spend **between $826 and $653,587** on incidents - *Accenture*

83% of SMBs are **not financially prepared** to recover from a cyber attack – *Cybercrime Magazine*

51% of SMBs have **no cybersecurity** measures in place at all - *Digital.com*

82% of ransomware attacks in 2021 were against companies with **fewer** than 1,000 employees – *ACA International*

55% of people in the U.S would be less likely to continue doing business with breached companies - *CNBC*

60% of SMBs **go out of business within six months** of falling victim to a data breach or cyber attack – *Cybercrime Magazine*

INDIVIDUALS & END-USERS

The Struggle to Keep Pace with Cybercriminal Sophistication

Cybersecurity measures in place by:

- **Individuals**
- Businesses,
- Governments,

are becoming ***obsolete*** by the growing ***sophistication*** of Cybercriminals

- World Economic Forum

33 Billion accounts will be breached in 2023 i.e. 2,328 daily, 97 victims per hour – *Astra Security*

1 Billion emails were exposed in a single year, affecting 1 in 5 internet users - *AAG IT*

217 Million users in the US were affected by data breaches in 2021 *- World Economic Forum*

95% of security breaches are attributed to human error *– World Economic Forum*

98% of cybercrimes rely on social engineering to accomplish successfully - *PurpleSec*

THE BATTLE

HACKERS

Underground Communities

Scripting
PowerShell
Bash

Programming
Python, C++, C, Java

Reverse Engineering

Vulnerability Exploitation

Network protocols
Routers, firewalls

Hacking Tools Proficiency

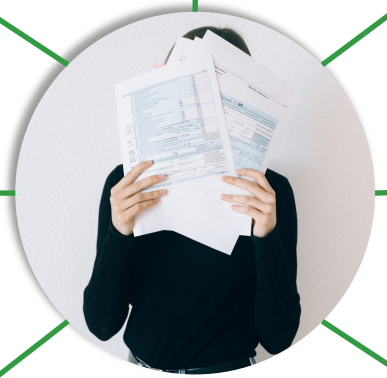
Social Engineering

AUDITORS

Risk Assessment

Analyse Processes

NIST, COBIT
ISO 27001
Frameworks



Analytical, Critical Thinking

Evaluate controls

Management Expertise

Audit & Assurance Methodologies

needs

Strong Technical Expertise

Duties of Directors & Legal Risks

Company Act of Mauritius 2001: the Board has a duty of care and a duty to act in the best interests of the company

Ensure compliance with:

- **All laws**
- Regulations
- Industry standards

Responsible to oversee the company's risk management framework and internal controls

Identify and assess risks :

- Implement relevant **controls**
- Monitor **regularly** the effectiveness of risk mitigation measures

Corporate governance

The Board has the option to seek:

- **Independent assurance**
- Regarding the effectiveness of risk management.

Protect Shareholders Interests

Protection objectives:

- Assets
- Information assets
- Data breach
- E-reputation
- Financial loss
- Loss of business

IT LEGAL LANDSCAPE

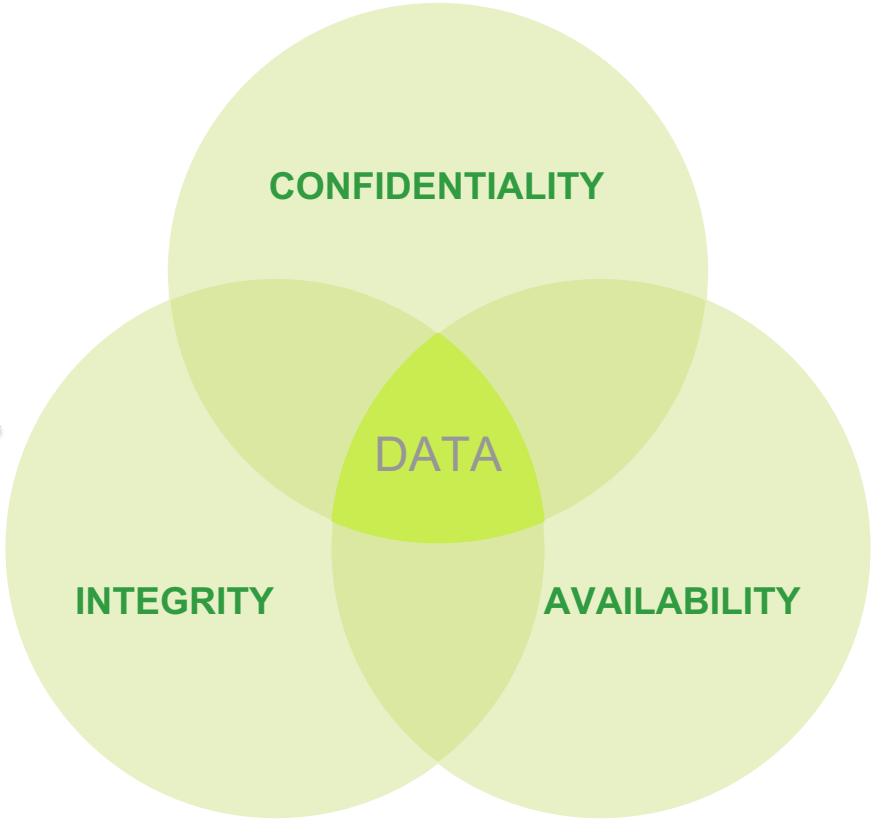
Compliance Risks for Organizations in Mauritius

Laws and regulations	Objectives of the Act	Legal Risks for Directors
Data Protection Act 2017	Addresses protection of personal data, regulates the collection, **processing**, storage, and transfer of personal data, ensuring individuals' rights are safeguarded.	Penalties, fines, and reputational damage Personal liability failing to implement appropriate data protection **measures**.
The Cybersecurity and Cybercrime Act 2021	Addresses offenses, such as unauthorized access to computer systems, **cyberbullying**, hacking, data interference, and computer-related fraud.	**Cybercrimes** committed by the company may lead to criminal charges, fines, and imprisonment.
Electronic Transactions Act 2001	Provides legal recognition and validity for electronic transactions, digital signatures, and **electronic records**	May result in contractual disputes, loss of legal validity, and **reputational harm** for the company
Financial Services Act 2007 and BoM / FSC guidelines	Includes provisions related to the security and **protection of financial data**, ensuring compliance with international standards and best practices	May face legal consequences for failing to implement appropriate **cybersecurity controls** in the financial services sector
ICT Act 2001	Regulates ICT licensing and details offenses related to **unauthorized access**, interception, or interference with computer systems or data, and provides for penalties.	Liable in case of unauthorized: **interception** of communication, access to data, disclosure of access code.

UNAUTHORIZED BREACH

Implications of Cyber Laws in Mauritius

Any Unauthorized Breach



Is an Offense

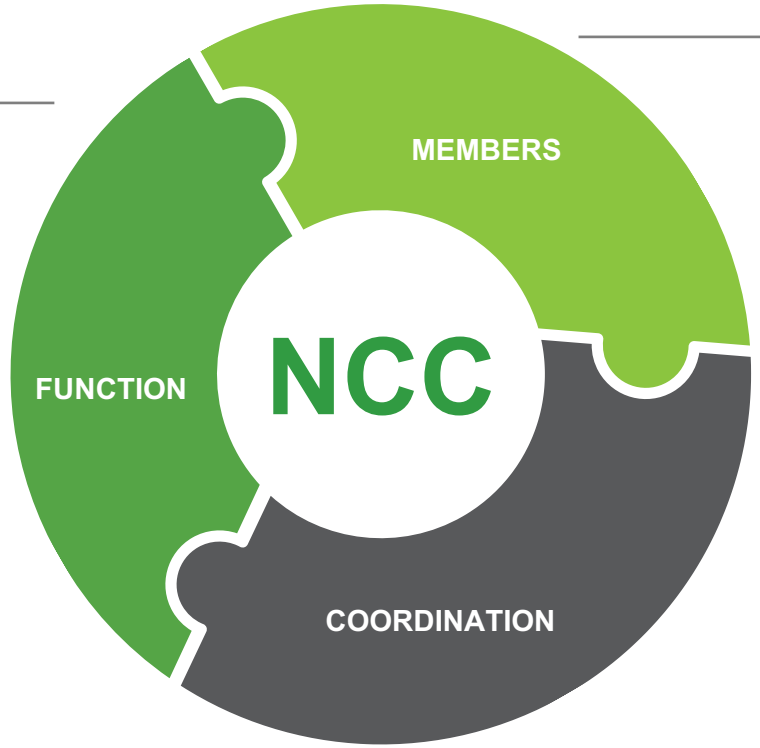
CIA Triad

TERMS OF REFERENCE

The National Cybersecurity Committee - NCC

Advisory:

- **Make recommendations** to the Government on cybersecurity and cybercrime.
- **Collect and analyse** information pertaining to cyberthreats
- **Analyse Cybersecurity** Reports.



Chairperson appointed by the Prime Minister

- PM Office
- Ministry of IT
- CERT-MU.
- DPO Office
- Mauritius Police Force
- Attorney General Office
- Bank of Mauritius
- Financial Service Commission
- Counter Terrorism Unit
- Private Sector
- Civil Society

Coordinate & Facilitate:

- **Security Framework** for the Critical Information Infrastructure .
- Cooperate with Incident Response Teams.
- Promote **capacity building** on prevention detection and cyber threats

CRITICAL INFRASTRUCTURE

Action Plan

Phase 1

Protect Mauritian Citizens in their day to day life

Objectives :

- Training program for students
- Training of Parents
- Personal and sensitive data
- How to protect you on-line
- Explain procedures, Fake profile, impersonation, Cyberbullying etc .

Phase 2

Critical Public Infrastructure affecting Citizens

Objectives :

- Banking Sector
- Telecommunications
- Government: All Ministries, secure IT infrastructure
- Utilities: CEB, CWA, Hospitals, Police, Fire-stations
- Transport: Airport, Metro, Maritime port

Phase 3

Pillar of economy

Objectives :

- Finance services Forex, Offshore sector
- Tourism
- Sugar
- Manufacturing
- Commerce
- BPO

FIGHTING HACKERS

How to get protected – Top 10

1. Use Strong, Unique Passwords:

Combine letters, numbers, and symbols.

Avoid using the same password for multiple accounts.

2. Enable Two-Factor Authentication (2FA):

Adds an extra layer of security beyond just passwords.

3. Keep Software Up-to-Date:

Regularly update operating systems, browsers, and applications.

4. Install Antivirus and Anti-Malware Software:

Ensure it is always active and regularly updated.

5. Be Wary of Phishing Scams:

Do not click on suspicious links or open unexpected email attachments.

6. Secure Your Wi-Fi Network:

Use strong encryption (WPA3 if available) and a complex password.

7. Backup Your Data Regularly:

Use both local and cloud-based solutions for backups.

8. Use a VPN for Public Wi-Fi:

Encrypts your internet connection on unsecured networks.

9. Limit Personal Information Sharing:

Be cautious about what you share online, especially on social media.

10. Educate Yourself Continuously:

Stay informed about the latest cybersecurity threats and best practices.

THANK YOU

Questions & Answers

Dr. Didier Samfat