# Cybersecurity Failures and Successes

*CPSI's 18th Public Sector Innovation Conference*

***August 2024***

***National Communications (ICT Security )***

state security

State Security Agency
REPUBLIC OF SOUTH AFRICA

# ICT SECURITY SERVICES

state security

State Security Agency
REPUBLIC OF SOUTH AFRICA

# ICT SECURITY SERVICE CATALOGUE

**Service (1) : ICT Security Risk and Assurance Services**

| SERVICE ELEMENT | DESCRIPTION |
|---|---|
| • Regular ICT Security Risk Assessments | • Determine security needs of the OoS<br>• Determine ICT Security Posture of OoS<br>• Monitor progress in the implementation of the security controls |
| • ICT Security Governance | • Develop ICT security standards and regulations<br>• Review of the ICT Security Policies, Standards, Processes and procedures. |

# ICT SECURITY SERVICE CATALOGUE

**Service (1) Name: ICT Security Risk and Assurance Services**

| SERVICE ELEMENT | DESCRIPTION |
|---|---|
| • Advisory Services | • ICT & Cyber Security Awareness Presentations & Advisory<br>• Evaluate compliance with security standards and regulations |

# ICT SECURITY SERVICE CATALOGUE

## Service (2) : ICT Security Monitoring Services

| SERVICE ELEMENT | DESCRIPTION |
|---|---|
| • Proactive Cybersecurity Services | • Alerts and Warnings<br>• Technology watch (Technology News, Security Updates, Cyber Crime and Intelligence in the News)<br>• Technical Vulnerability Assessment and Penetration Testing<br>• Monitoring (Incident Management)<br>• Cyber Threat Intelligence |

# PRESENTATION OBJECTIVE

- To provide an overview of Cybersecurity Failures and Successes
- Provide an overview of South Africa's own ICT security posture

# Introduction to Cybersecurity

- **Definition:** Protection of internet-connected systems, including hardware, software, and data, from cyberattacks.

# Importance of Cybersecurity

**Why Cybersecurity Matters**

- Protects sensitive data against unauthorised access and/or modification
- Maintains business continuity
- Safeguards reputation and trust

**Consequences of Cybersecurity Failures**

- Financial loss
- Loss of confidence
- Legal consequences
- Reputational damage

# Evolution of Cybersecurity

- **Early Days:** Focus on antivirus software and firewalls.
- **Modern Cybersecurity:** Advanced threat detection, AI-driven responses, and zero-trust architectures.
- **Growing Threat Landscape:** From viruses and worms to ransomware and nation-state attacks.

# Top 16 Cybersecurity Threats in 2024

1. Social Engineering
2. Third-Party Exposure
3. Configuration Mistakes
4. Artificial Intelligence Cyber Threats
5. DNS Tunneling
6. Insider Threats
7. State Sponsored Attacks
8. Ransomware
9. Trojan Horses
10. Drive By Cyber Attack
11. Poor Cyber Security Hygiene
12. Cloud Vulnerabilities
13. Mobile Device Vulnerabilities
14. Internet of Things
15. Poor Data Management
16. Inadequate Post-Attack Procedures

# What do hackers want?

1. Disrupt business functions
2. To influence the political, legislative and economic direction
3. To steal state information
4. To steal Intellectual Property
5. To have competitive advantage
6. To have command and control
7. Financial gain
8. For fun and practice

# Notable Cybersecurity Successes

**1. The Takedown of Emotet (2021)**

- **Details:** International effort led by Europol to dismantle one of the most dangerous malware botnets.
  - email attachment
  - Was sold to other cyber criminals
  - Had a run of over 5 years
  - Took multinational collaboration to take down
- **Impact:** Severely disrupted global cybercrime activities.

**2. Containment of the WannaCry Ransomware (2017)**

- **Details:**
  - Targeted Microsoft Windows OS
  - Propagated using an Exploit, EternalBlue, developed by National Security Agency
  - Ethernet was stolen a month prior to the attack
  - Microsoft issued a patch and those who did not apply the patches or were using unsupported OS remained vulnerable
    - Quick identification of a kill switch by a security researcher prevented the spread of the ransomware. The spread was contained within 8 hours of identification
- **Impact**: Saved countless organizations from data loss and financial damage.

# Notable Cybersecurity Successes

## 3. Advanced Encryption and Secure Communications

- **Details:** Widespread adoption of HTTPS and end-to-end encryption in communications.
- **Impact:** Enhanced privacy and security for users across the globe.

# Case Studies in Cybersecurity Failures

- **1. Equifax Data Breach (2017)**
  - **Details:** Hackers exploited a vulnerability to access sensitive data of 147 million people.
  - **Failure:** Lack of timely patching and inadequate security measures.
  - **Impact:** Significant financial losses and loss of consumer trust.

- **2. SolarWinds Attack (2020)**
  - **Details**: Nation-state attackers inserted a backdoor into SolarWinds' software update.
  - **Failure:** Insufficient supply chain security and delayed detection.
  - **Impact:** Compromise of numerous U.S. government agencies and large corporations.

- **3. CrowdStrike's Falkon (2024)**
  - **Details:** A botched Software update caused the biggest outage in history
  - **Failure: Configuration** update was not compatable with Microsft Operating systems
  - **Impact:** 8.5 million systems crushed and were unable to restart, causing disruption of critical services worldwide.

# Lessons Learned from Failures

- **Importance of Timely Patching:** Regular updates to software and systems to close vulnerabilities.
- **Strengthening Supply Chain Security:** Monitoring and securing third-party vendors.
- **Continuous Monitoring and Incident Response:** Proactive measures to detect and mitigate threats early.
- **User Awareness and Training:** Educating employees and users on recognizing and avoiding cyber threats.

# How are we doing as RSA

- Due to little to no innovation in the country, South Africa remains a consumer and not developer of technology, this exposes us to 3rd Party risks
- Inadequate security skills in the country
- Remuneration of skilled person remain below world standards
- Security consciousness remains very low

# Most Common Incidents in Government

- Ransomware
- Unauthorized financial transactions
- Denial of Service attacks
- Suspicious URL and Domain Impersonating key entities
- Compromised email accounts and email phishing
- Multiple instances or records listed for sale on an illicit underground marketplaces

# Common deficiencies in government

- Poor policy implementation, compliance enforcement and security awareness
- Poor Security Hygiene – email security, endpoint security, unsupported software, preservation of system log
- Inadequate Patch Management & Hardening

# Common deficiencies in government

- Incident Management
- Change management control
- Business Continuity Management
- Third party management
- Poor access management

# Strategies for Future Success

- **Adoption of Zero-Trust Models:** Never trust, always verify.
- **Artificial Intelligence and Machine Learning:** Leveraging AI/ML for threat detection and response.
- **Collaborative Defense:** Sharing threat intelligence among organizations and nations.
- **Regulatory Compliance:** Adherence to global cybersecurity standards and regulations.

# Conclusion

- **Summary:** Cybersecurity is a dynamic field with successes and failures providing critical lessons.

- **Final Thoughts:** Continuous evolution, vigilance, and collaboration are key to securing the digital future.

# THANK YOU