CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

NATIONAL CYBER SECURITY AWARENESS

DIGITAL FINANCIAL SERVICES:- Cyber Landscape in DFS

PRESENTED BY

Sinaye Dlamini
Head ICT
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Presentation Outline

- Emerging Trends in DFS
- Top 5 Cybersecurity threats for the ICT Industry
- Mitigation Strategies
- Financial Services Sector strategic initiatives
- Country specific risk/threat minimizing initiatives

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Emerging Trends in DFS

Let there be no mistake about it: Cyber threats and risks of serious breaches are not going anywhere!!!

- Growth in mobile apps and web portals creating more security risk exposures
- The growth of FinTech… and a demand pull for open banking and APIs
- Increasing Consumer and Data Protection… POPI Act in SA, EU GDPR, DPA in UK….. Demand for more data privacy
- Third parties continue to be a target… major banking cyber attacks due to vulnerabilities in shared banking systems & third party networks… $81 million heist from Bangladesh Bank by exploiting a vulnerability in a shared banking system called SWIFT
- Increase in cyber resilience guidelines and supervision for financial institutions
- AI and machine learning tools used for both threat detection and by threat actors to carry out advanced sophisticated attacks

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Top 5 Cybersecurity Threats

Top Threats	Year						
	2018	2017	2016	2015	2014	2013	2012
Malware	1	1	1	1	1	2	2
Web-Based Attacks *	2	2	2	2	2	1	1
Web Application Attacks **	3	3	3	3	3	3	3
Phishing	4	4	6	8	7	9	7
Denial of Service	5	6	4				
Spam	6	5	7				

Source: Eutelsat Communications (ETL) Annual Report

* Most common threat for financial attacks
** Government and financial institution apps are particularly popular targets

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Cybersecurity Threats

MORE RECENT DEVELOPMENTS

- Credential and identity theft
- Data theft and manipulation
- Disruptive and destructive malware
- Emerging technologies: Blockchain, Cryptocurrency and Artificial Intelligence
- Disinformation

Source: AccentureSecurity – Future Cyber Threats

Cybersecurity Threats – Close Up

- "SA Banks hit with ransom-driven cyber attack" – eNCA, 25 Oct 2019
- "South Africa is under attack" – myBroadBand, 28 Oct 2019
- "City of Joburg shuts down all systems after cyber attack demanding bitcoin ransom"- news24, 25 Oct 2019

WARNING! - The files on THE COMPUTERS IN YOUR ACTIVE DIRECTORY have been encrypted!!! To decrypt ALL files, on THE ALL COMPUTERS you have to pay 5 BTC *(five bitcoins)* to address 1MXaQnAuYwuuhEyabPrAN6aq5cjQxvKhAi within 48 hours, or ALL FILES will be lost for good!
Your ID is 000012684496. Upon successful transaction send your ID as subject at johny.walker55664@offensivelytolerant.com and you will receive a key with decrypting instructions! Before you pay, you can send one file up to 2 MB to be decrypted as a proof.

Lack of information sharing on incidents

Mitigation Strategies

How to avoid cybersecurity threats? Stay alert, stay proactive

- The best defense against such innovative threats is often simply practicing good cyber-hygiene (like avoiding clicking on suspicious links or attachments from unknown users), and having a strong defense system (like using firewalls, intrusion detection, and prevention systems).
- Proper training and awareness sessions for the staff and the security teams can also help you turn away any intrusion attempts made by bad actors.
- Having a proactive threat intelligence system can help you keep your organization one step ahead of such cybersecurity threats.

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Mitigation Strategies

- Education of potential targets about fake mail, random clicking and oversharing of personal information
- Patching vulnerabilities and filtering web traffic
- Reaction planning, ISP with DoS protection and organization specific protections such firewalls and access lists
- Defining policies for secure app development and for the authentication and validation of mechanisms
- Spam filters
- Encryption and reduction of access rights
- User awareness, in addition to segregation of duties and limiting access to data

Financial Services Sector Strategies

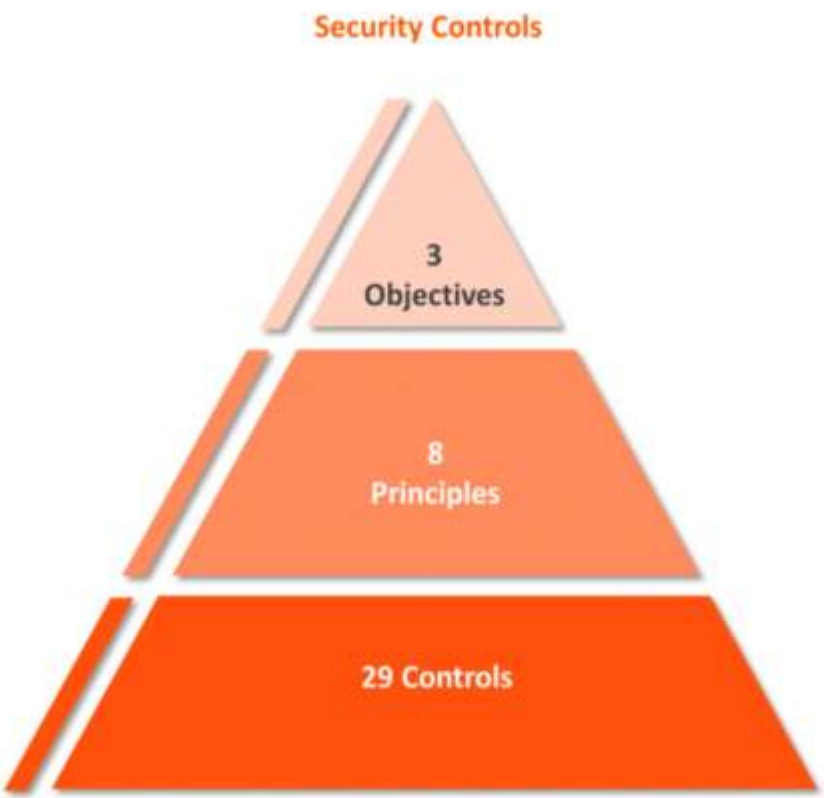
- Bank of International Settlements (BIS) initiatives; *Guidance on cyber resilience for financial market infrastructures*: provides guidance on the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities in order to limit the escalating risks that cyber threats pose to financial stability.

- Organization specific policies based on NIST Cybersecurity Framework or ISO 27001 standard

Financial Services Sector Strategies

- The Society for Worldwide Interbank Financial Telecommunication (SWIFT)initiatives; SWIFT Customer Security Programme (CSP)

CSP | Secure and Protect – Customer Security Controls Framework **v2019**



CSP Security Controls Framework (combines 1 & 2)		
Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Eswatini & CBE Strategies

- Cyber Resilience Framework
- Cyber Incident Response Plan
- Information Security & Cyber Security Policies
- Information Security Management System – ISO 27001 & ISO27032 based
- Continuous User Awareness & Training initiatives
- Penetration Testing & Vulnerability Scans

- *Cyber Security guidelines for supervised institutions*
- *Financial Institution oversight for compliance to SWIFT CSP Mandatory Controls*
- *Cyber Security Operations Centre*
- *Financial Sector Cyber Incident Response Team*

CENTRAL BANK OF ESWATINI
Umntsholi Wemaswati

Key Take-Away

- Preparedness
- Information sharing
- Developed & dedicated cyber security competencies

Quotable Quote

"When it comes to getting hacked – it is not a question of how you can prevent it or if it will ever happen at all. Because no matter the precautions your team takes, it will be a matter of WHEN will it happen. And an even bigger question is what will be done about it?"

END