SANLAM AS A CASE STUDY

Mike O’Donovan

Chief Executive: SEB Platform Solutions

Insurance | Financial Planning | Retirement | Investments | Wealth
Evolving to a FinTech organisation:

- Digitisation of engagement models
- Automation of processes
- Data & analytics
- Artificial Intelligence
A DATA DRIVEN ENVIRONMENT
Evolving to a FinTech organisation:

Clients demand more information (data):
- To better service and advise clients,
- Reports & information
- Tools & models to test scenario outcomes,
- Statistics & analytics

Needs to be: accessible, anywhere, anytime, anyhow – typically web-based

Regulators require providers to hold more data:
- FSCA driving more direct communication with members for retirement funds & TCF
- PPR requirements – long-term insurance compels member level communication
- Providers required to hold more member level details
PRINCIPLE 12 OF THE KING IV REPORT ON CORPORATE GOVERNANCE:
Covers the responsible governance of information and technology within an organisation.

CYBERCRIME BILL (PENDING), THAT BUILD ON CHAPTER XIII OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002:
Includes the codification and imposition of penalties on cybercrimes, and demands more vigilance on the part of organisations in how they protect those whose data they hold from cybercrimes.

PROTECTION OF PERSONAL INFORMATION ACT, 2013 (OR POPI):
Looks at the safeguarding of personal information held by public and private bodies.

FINANCIAL SECTOR REGULATION ACT 9 OF 2017 (TWIN PEAKS):
○ Prudential authority = enforcement of regulations, compliance, risk management (business & information technology),
○ FSCA = to deter misconduct, protect consumers.
FINANCIAL SECTOR A TARGET
MOTIVES
Cyber criminals looking to monetise data

- To hold organisations to ransom
- Commit fraudulent transactions
- Identity theft
- On-sell personal data
- On-sell of system access
- Protest or propagating a cause or idealism
HOW
Cyber criminals looking to monetise data

- Hacking of websites & web-based systems
- Viruses, ransomware, malware
- Email spamming, web phishing, malvertising
- Vishing & spear phishing
- WhatsApp
HOW
Cyber criminals looking to monetise data

- Theft of hardware, laptops, flash drives, external hard drives
- Interception of data transfers
- Cyber forgery
- Cryptojacking
ATTACKERS ARE WELL ORGANISED
SO...
WHAT DO WE DO?
SANLAM’S FOCUS

Governance Frameworks & Policies
Internal Physical Environment
Data Management
External Environment
Testing
GOVERNANCE STRUCTURES
Sanlam’s focus

Formal Policies & Frameworks
- Information governance, information security, end-user computing

Governance Oversight & Reporting
- Risk forums, internal business reports, external assurance reports, incident reporting,

Risk Assessments:
- Crown jewels & controls aligned to the centre for internet security’s (CIS) top 20 list of prioritised information security controls

Cyber Security Response Capabilities
- Cyber security incident response team (CSIRT)
- Forensic capability
- Data recovery competency

Formalise, test and improve preventative controls in line with Cyber Intelligence (CI) security
INTERNAL ENVIRONMENT
Sanlam’s focus

Company Asset Management
- Hardware and software assets and ownership

Private Devices
- Inventory of authorised and un-authorised devices (mobile devices & Wi-Fi)

Device Management
- Local administration & data protection
- Encryption and ports blocking (PC, laptops, external hard drives, flash-drives)

Access Management
- Logical & physical access
- Controlled use of administrator privileges
- Privileged accounts management
- Physical data center security
DATA PROTECTION
Sanlam's focus

Encryption of Data Transfers
- Emails
- FTP
- Password protected files (spreadsheets !)

Data Discovery and Data Leakage Prevention
- Monitoring irregular behavior, listening technology, audits
- Code changes

Structured Data Management
- Access to data & databases (processing portfolios, reports etc.)

Unstructured Data
- Ownership and access management (housekeeping)
EXTERNAL ENVIRONMENT
Sanlam’s focus

Boundary Defense:
- Identity access management (IAM), firewalls
- Limitation and control of network ports

Software Applications:
- Application software security (penetration testing at a database level, patches & updates)
- Malware defences

Vendor Solutions:
- Outsourced hosting arrangements
- Third party developed deployments
TESTING OF CYBER CAPABILITIES
Sanlam’s focus

**Desktop exercises**
- user training & awareness

**Simulations**
- DR & BCP exercises
- Incident simulations

**Technical tests**
- actual attacks to test detection and response capabilities
CYBER TEAMS
What does Sanlam do

**Red Team:**
- Hackers that continuously try and break into systems
- Assist the blue team in addressing vulnerabilities

**Blue Team:**
- Focus on defense
- Preventative controls
- Cyber intelligence capabilities
- Detection & listening – early warning system *(like a neighborhood watch)*
- Monitor internal security events *(preserve the events in a forensically sound way and correlate events to identify threats)*
- Incident response
- Monitor internal security events *(preserve the events in a forensically sound way and correlate events to identify threats)*
SANLAM GROUP CYBER RESILIENCE FRAMEWORK
Sanlam’s response

Governance
- Cyber Strategy & Budget
- Regulatory Watch
- Staffing
- Resilience Assessment
- Cyber & Security skills assessment & Training
- Assurance Reporting
- Security Awareness
- Risk Management
- Performance Management
- Sourcing

Early Warning
- Cyber Intelligence Management

Monitoring
- Maintenance, Monitoring & Analysis of Audit Logs

Response
- Cyber Crisis Management
- Incident Response & Management
- Data Recovery Capability
- Cyber Forensics

Basis of Information Security Capabilities & Control

Prevent
- Device Inventory
- Software Inventory
- Secure Configuration of Mobiles, Desktops & Servers

Detect
- Vulnerability Assessment & Remediation
- Administration Privileges
- Malware Defence

Deny
- Email & Web Browser Protection
- Network Ports, Protocols & Services
- Boundary Defence

Disrupt
- Secure Configuration of Firewalls, Routers & Switches
- Data Protection
- Controlled Access

Degrade
- Application Software Security
- Account Monitoring & Control
- Wireless Access Control

Deceive
- Penetration Testing
- Advanced Threat Detection

Destroy
- Application Software Security
- Penetration Testing
- Advanced Threat Detection
SO, WHAT SHOULD YOU DO?

Your responsibility

- Do you know how the data that you are the custodians of is stored, managed and governed?
- Is your own environment safe?
- How to you handle data between your clients, administrators, funds and service providers?
- Have you completed the cyber security checklist as part of you service provider assessment?