2018

Innovation and Cybersecurity **Conference**

28–30 August 2018

Coordinating efforts, **establishing response** structures, and **creating** regulatory certainty in a **disruptive environment** where **innovation** and cyber converge

South African Reserve Bank

Cyber Threat Landscape

Risk management practices, controls and defenses

Nida Davis: Associate Director, Supervision and Regulation Division

Federal Reserve Board of Governors – Washington D.C.

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any agency of the U.S. government. Examples of analysis performed within this article are only examples. They should not be utilized in real-world analytic products as they are based only on very limited and dated open source information. Assumptions made within the analysis are not reflective of the position of any U.S. government entity.

Growing Cyber Threats / Risks to Financial Sector

- **Persistent Threats (APTs) – Cyber Crime / Large Scale Cyber Attacks**
  - Sophisticated hackers, hacktivists, and nation state groups that display a high level of technical expertise.
  - Longer dwell time in network increases time to conduct damage.*
  - Well-coordinated and resourced.

- **Interconnectedness Risks - 3rd and 4th Party Risks / Failure of Wider Infrastructure**
  - Multiple vendors, partners and other parties provide more touch points or opportunities for threat actors and malware to gain access.
  - Supply chain compromises.

- **Social Engineering – Identity Theft / Data Breaches**
  - A tactic, often relying on human interaction, to bypass cyber security standards.
  - Can be non-technical (threat actor led fraud / intrusion).
  - Can allow threat actors to gain authorized access to network.

** Dwell time represents the number of days that a threat "lives" in a system before detection or ultimate remediation*

South African Reserve Bank

Growing Cyber Threats/Risks to Financial Sector

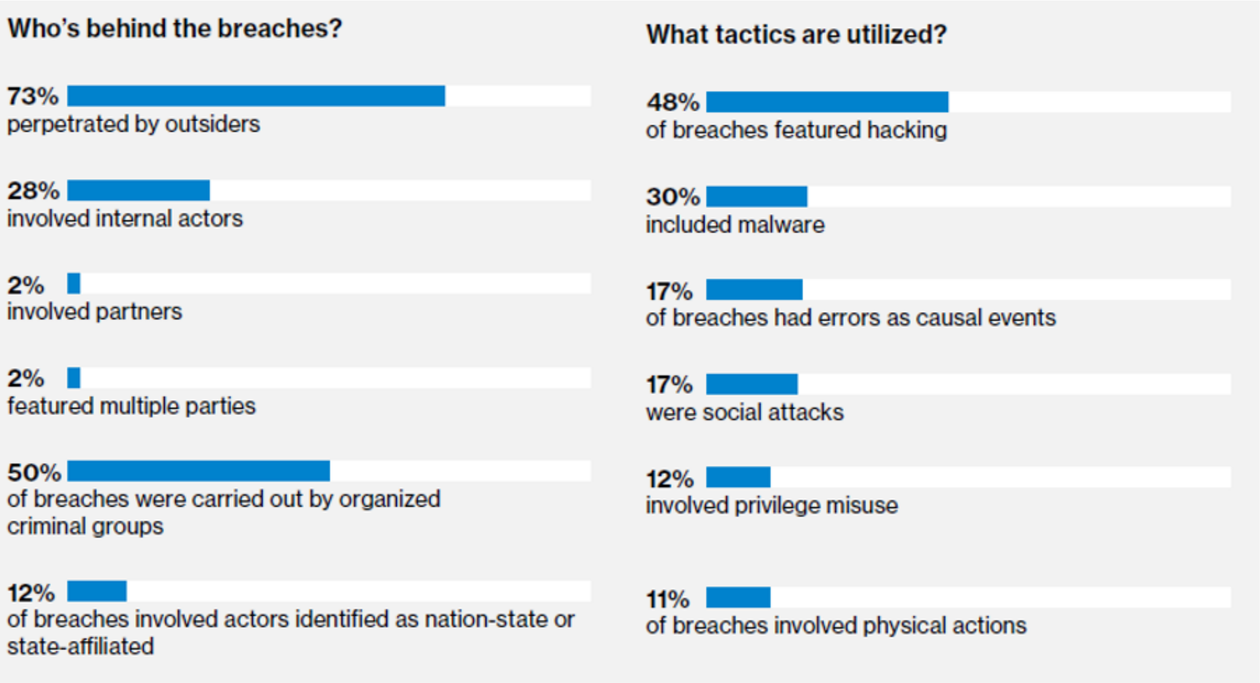
- **End-Point Security (IoT) / Chip Vulnerabilities**
  - Increasingly expanding proliferation of end-point devices whose security is not well understood, not well configured, or not well hardened.
  - New class of chip vulnerabilities that exploit the fundamental design of processors.
  - Fileless attacks are growing at an alarming rate (malware is stored in the RAM to evade detection).
  - *Meltdown* and *Spectre* were the first identified chip vulnerabilities, but new chip vulnerabilities are being discovered regularly.

- **New and Evolving Malware**
  - Threat actors and malware developers are constantly developing new malware and developing new variants of known malware to increase capabilities and tailor for specific targets.

- **Software Development Vulnerabilities**
  - Threat actors are constantly developing new tactics, techniques, and processes to exploit security flaws in poorly developed software.

South African Reserve Bank

Financial Sector Breaches by the Numbers



Who's behind the breaches?

73%
perpetrated by outsiders

28%
involved internal actors

2%
involved partners

2%
featured multiple parties

50%
of breaches were carried out by organized criminal groups

12%
of breaches involved actors identified as nation-state or state-affiliated

What tactics are utilized?

48%
of breaches featured hacking

30%
included malware

17%
of breaches had errors as causal events

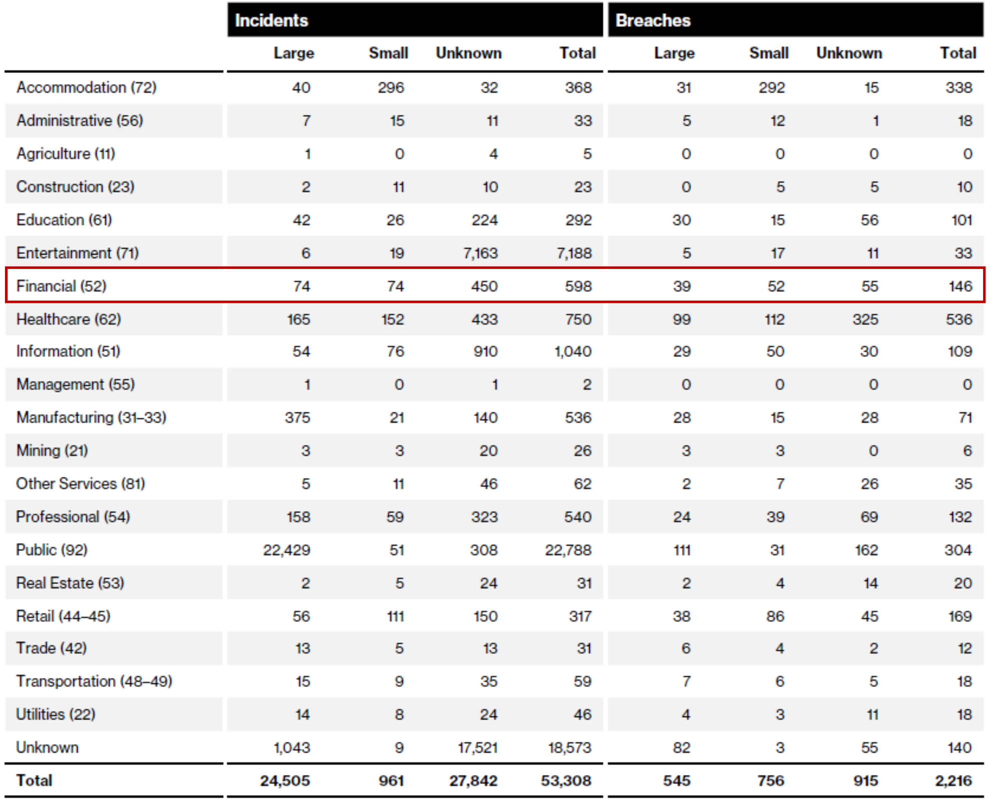
17%
were social attacks

12%
involved privilege misuse

11%
of breaches involved physical actions

** Data pulled from the 2018 Verizon Data Breach Investigation Report*

Financial Sector Incidents in Perspective



	Incidents				Breaches			
	Large	Small	Unknown	Total	Large	Small	Unknown	Total
Accommodation (72)	40	296	32	368	31	292	15	338
Administrative (56)	7	15	11	33	5	12	1	18
Agriculture (11)	1	0	4	5	0	0	0	0
Construction (23)	2	11	10	23	0	5	5	10
Education (61)	42	26	224	292	30	15	56	101
Entertainment (71)	6	19	7,163	7,188	5	17	11	33
Financial (52)	74	74	450	598	39	52	55	146
Healthcare (62)	165	152	433	750	99	112	325	536
Information (51)	54	76	910	1,040	29	50	30	109
Management (55)	1	0	1	2	0	0	0	0
Manufacturing (31–33)	375	21	140	536	28	15	28	71
Mining (21)	3	3	20	26	3	3	0	6
Other Services (81)	5	11	46	62	2	7	26	35
Professional (54)	158	59	323	540	24	39	69	132
Public (92)	22,429	51	308	22,788	111	31	162	304
Real Estate (53)	2	5	24	31	2	4	14	20
Retail (44–45)	56	111	150	317	38	86	45	169
Trade (42)	13	5	13	31	6	4	2	12
Transportation (48–49)	15	9	35	59	7	6	5	18
Utilities (22)	14	8	24	46	4	3	11	18
Unknown	1,043	9	17,521	18,573	82	3	55	140
Total	**24,505**	**961**	**27,842**	**53,308**	**545**	**756**	**915**	**2,216**

** Data pulled from the 2018 Verizon Data Breach Investigation Report*

The Expanding Role of the CISOs

- **Assess Cybersecurity Risks:** CISOs keep senior leadership and the Board updated regularly on cybersecurity risks and make sure that effective cybersecurity defenses are a top priority.
- **Implement Cybersecurity Programs:** CISOs are responsible for implementing cybersecurity programs / frameworks. Although there is no authoritative framework for cybersecurity in the financial sector, 91% of all companies that have adopted a standard security framework have either adopted NIST CSF or ISO/IEC 27001/27002.*
- **Promote Cybersecurity Awareness Culture:** Establish cybersecurity training programs and promote cybersecurity awareness.
- **Balance Competing Priorities:** CISOs surveyed were split on their top priorities for securing their organizations against cyberattacks.*
  - 35% said that employee training is a top priority for improving security posture in the financial sector.
  - 25% said that infrastructure upgrades and network defense are the top priority.
  - 17% said that breach prevention is the top priority.

*"The role of the modern day CISO is to provide the leadership and guidance necessary for an organization to manage the risks to the confidentiality, integrity and availability of the organization's intellectual property and information technology assets."***

*** Infosec Today*

** Survey was conducted by FS-ISAC in 2018 and polled current CISOs of member organizations.*

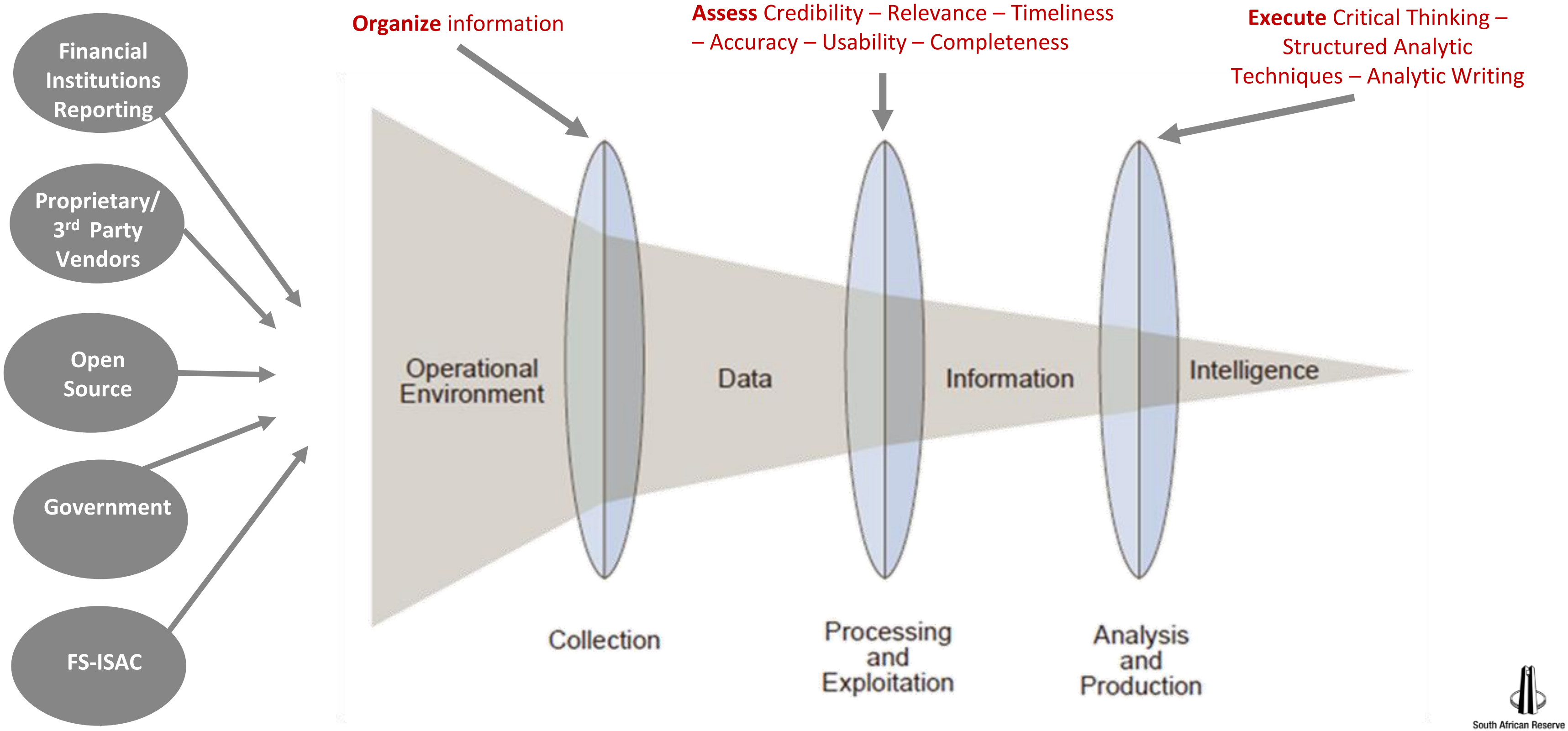
The Expanding Role of Cyber Threat Intelligence

- Financial institutions, depending on their size and complexity, should consider establishing internal threat intelligence teams that monitor the cyber threat landscape and share with their peer groups.

- Since smaller banks sometimes lack internal resources to maintain awareness of cyber threats, they can participate in cyber information sharing efforts such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC).

- While it is sometimes hard to get actionable information declassified, government agencies typically work with the sector to disseminate actionable intelligence to the sector. Engage and partner with your cyber threat intelligence government agencies as appropriate.

Cyber Situational Awareness / Threat Intelligence



Organize information

Assess Credibility – Relevance – Timeliness – Accuracy – Usability – Completeness

Execute Critical Thinking – Structured Analytic Techniques – Analytic Writing

Effectively Managing and Mitigating Cyber Risks

- **Strengthen Cybersecurity Governance:** Establish clear and effective 3LOD risk management structure. Clearly define roles and responsibilities for staff implementing, managing and overseeing the effectiveness of the cybersecurity strategy and cybersecurity framework to ensure accountability. Provide adequate resources, appropriate authority, and access to the governing authority (e.g., board of directors or senior officials at public authorities). Establish a clear separation of concern along the 3LOD model for risk, audit and operations.

- **Ensure Cyber Resilience Readiness:** Review the cybersecurity strategy and framework / controls regularly and when events warrant — including cybersecurity governance, risk and controls assessments, monitoring, response, recovery and information sharing components — to address changes in cyber risks, allocate resources, identify and remediate gaps and incorporate lessons learned.

- **Test Cyber Resilience Readiness:** Assess cyber resilience readiness by executing cybersecurity incident drills, business continuity and disaster recovery exercises and tabletop exercises to stress-test organizational cyber resilience readiness. Based on risk, consider the use of Threat Led Penetration Testing (TLPT) where appropriate.

South African Reserve Bank

Effectively Managing and Mitigating Cyber Risks

- **Adopt Layered Security Defenses:** Identify, classify and protect critical assets, systems and data. Establish systematic infrastructure, systems and data monitoring capabilities to rapidly detect cyber incidents. Periodically evaluate the effectiveness of controls, including enterprise architecture, network and infrastructure monitoring, secure software development, infrastructure configuration testing, audits and exercises.

- **Know Your Connections:** Identify critical functions, activities, products and services, including interconnections, dependencies and third parties. Prioritize their relative importance and assess their respective cyber risks. Identify and implement security controls – including systems, policies, procedures and training – to protect against and manage those risks within the tolerance set by the governing authority.

- **Respond Quickly:** Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators and other public authorities, as well as shareholders, third-party service providers and customers as appropriate); and (d) coordinate joint response activities as needed.

Effectively Managing and Mitigating Cyber Risks

- **Resume Operations Responsibly:** Allow for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

- **Leverage Threat Intelligence Capabilities:** Institutions are increasingly leveraging threat intelligence built on peer relationships and public-private partnerships to remain responsive to emerging threats.

- **Engage in Public-Private Collaboration:** Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents and responses to enhance defenses, limit damage, increase situational awareness and broaden learning.

**PwC. "Global State of Information Security Survey 2016." 9 October 2015*.

South African Reserve Bank

Use Layered Security Controls/Defenses

- **Layered security controls include but are not limited to the following:**
  - ✓ **Access and Identity Management:** Implement the principle of least privilege, including protection of administrative privilege, to combat compromise of administrative credentials and establishment of persistence.
  - ✓ **Multifactor Authentication:** Implement rigorous authentication and authorization processes to combat credential theft.
  - ✓ **System and Network Segmentation**: Implement the principle of least access to combat lateral movement.
  - ✓ **Endpoint Security:** Implement detection and mitigation of anomalous system behavior to help combat malware.
  - ✓ **Data Encryption:** Implement data encryption at rest and in transit to reduce the risk of data theft.
  - ✓ **Secure Software Assurance:** Implement a secure software assurance program to mitigate the threat of exploitation of software vulnerabilities.

Steps to Prevent or Minimize Disruption

Operational Readiness: Assessment of an institution's cybersecurity controls and governance is an important step towards improving its ability to identify, detect, respond, recover and reduce the impact of major cyber incidents. When assessing your cybersecurity posture:

- Establish clear operational availability and operational readiness objectives.
- Set and communicate operational readiness objectives, manage expectations and establish operational readiness processes at all levels of the organization.
- Develop well defined cybersecurity incident management and response procedures and communication plans (playbooks / protocols).
- Maintain and continue to update a diverse set of operational resilience best practices to ensure operational readiness capabilities that include people, processes and culture.
- Report early, clearly and objectively operational disruption findings caused by cybersecurity incidents, and formulate concrete remedial actions.
- Ensure cybersecurity operational readiness assessments are reliable and fair.
- Develop an after action plan and ensure follow up and implementation of mitigating controls.
- Make sure to contact your regulator and report cybersecurity incidents.

Mitigating Growing Cyber Threats/Risks

Persistent Threats (APTs)

- Monitoring for application & infrastructure changes, data access attempts and data transfers.
- Early identification is key to minimize damage (suspicious connections, emails, traffic, etc.).
- Data encryption at rest and in transit.
- Robust incident management planning.
- Proactive threat intelligence / monitoring of alerts.
- Backups (online and offline).
- Emergency response and recovery readiness

Insecure 3rd / 4th Party Services

- Legal agreements with clear SLAs and NDAs governing 3rd party services, including the use of 4th party service providers.
- Cybersecurity assurance prior to establishing integration of 3rd party services.
- Testing and patch management.
- Proactive threat intelligence before compromise.
- Robust incident management planning.
- Backups (online and offline).

Social Engineering

- Training and testing for awareness and prevention.
- Layered defense coupled with identity and access management.
- Threat intelligence for informing users about current social engineering lures and tactics, techniques and procedures (TTPs).

South African Reserve Bank

Mitigating Growing Cyber Threats/Risks

End-Point Security (IoT) / Chip Vulnerabilities

- Asset management to ensure awareness of hardware and software components and weigh the risks of the components appropriately.
- Patch management.
- Vulnerability assessment and penetration testing.
- Threat intelligence and vulnerability management.

New and Evolving Malware

- Prevention through user training and up to date anti-virus software.
- Patch management.
- Proactive threat intelligence.
- Robust incident management planning.
- Monitoring Cyber alerts.

Software Development Vulnerabilities

- Prevention through secure coding programs.
- Penetration testing and scanning for software vulnerabilities.

Emerging Cyber Threats

Questions?

South African Reserve Bank