2018 RSA CONFERENCE SFO

CONFERENCE FEEDBACK

DEVEN GENGAN

CONTENTS

- Preamble
  - What is the RSA conference about ?
- Industry Trends
  - 2018 Trends
- Before the Conference
  - Some personal care…mindset adjustments
  - My thinking before I went…
- After the Conference
  - My thinking after I went…
- Keynotes
  - Best keynote
- Sessions
  - NIST Cybersecurity Framework on a page
  - How to beat MBAs at their own game on a page
  - Homomorphic encryption on a page
- Products
  - BayDynamics | Beyond Security | Guardicore | F5 Networks | Axonius | Firemon

PREAMBLE

WHAT IS THE RSA CONFERENCE ABOUT ?

- $\approx 42\,000\ attendees$
- Mix : Keynotes, P2P, tracks, tutorials, expo floors, seminars
- @scale…. 17 Keynotes, 700 speakers, 550+ sessions and 600+ companies on the expo floor

- So…., you really had to read, critically think and plan before the event
- Seats full up quick, meaning it was important to book well before the event so that you get a space in the sessions
- The event is broad, covering all aspects of Cybersecurity. This was one of the main reasons for me attending so that I could get an overview of the body of knowledge, product sets and "go deep" into areas of interest
- Information Security vs Cybersecurity ??

INDUSTRY TRENDS

NON-EXHAUSTIVE (DSS)

2018 TRENDS …..

- AI-powered attacks
  - Helps in info gathering, trick AI solutions etc…
- Sandbox aware malware
  - They can “sense” and only execute code when outside
- Ransomware and IoWhat ?
  - No regulating body
  - Known for weak security and Alexia does go loco sometimes [*Youtube*]
- General Data Protection Regulation (GDPR)
  - The “maritime law of IT” , if the ship has the flag then those laws apply in international waters [*Zuckerberg, M., Senate Committee, USA, 2018*]
- Poor uptake of Multi-Factor Authentication (MFA) solutions
  - Often user experience tips the scale
- Adoption of more sophisticated security technologies such as:
  - Deception technology : Honeypots, honeytokens trapping attackers
  - Detect & Respond to anomalous behaviour: Endpoint detection and response, network traffic analysis
  - Realtime change auditing solutions: detect and respond to user privilege abuse and suspici activity…account modifications etc..
- Advanced Persistent Threat (APT’s), often State sponsored
  - http://map.norsecorp.com

One of the citations is an attempt at humor

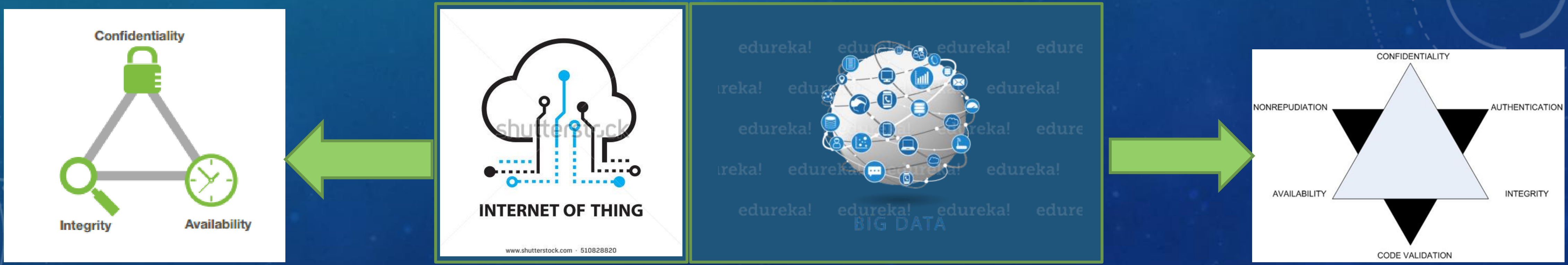
BEFORE THE CONFERENCE

SOME PERSONAL CARE…MINDSET ADJUSTMENTS

- Zen moments…, sleep is also a form of meditation, running, swap hash browns for fruit…always !!
- Clear the fog and filter out snake oil sales….usual suspects: AI, Machine Learning, Blockchain
- Get conference tag etc the day before
- Re check agenda and booked sessions on the app, then read the app was compromised …. really…umm…2011..SecureID…
- Finish up some last minute reading on homomorphic encryption
- Mute WhatsApp and Telegram

MY THINKING *BEFORE* I WENT…

- Easy to digest and get buy-in threat intelligence
  - Board level… who is attacking us, for what purpose ?
  - Can we learn their tactics, techniques and procedures ?
  - Darkweb, fraudulent websites, credentials theft and selling, 3rd party impacts to our organization
- Integrated security platforms
  - #whatalotigot
  - Endpoint security, malware sandboxes, machine learning (point solutioning) vs **integrated** threat ***defence***
  - Security Operations and Analytics Platform Architectures (SOAPA)…IBM QRADAR, SPLUNK..
    - Key: heterogeneous architectures, APIs, open-source vs proprietary agendas
- Approaching/refactoring -> Business Risk perspective
  - Basics of CISSP, SABSA, NIST Cybersecurity Framework



MY THINKING *BEFORE* I WENT…

- The perimeter left the building in 2008 for me….
  - SAML 2.0, Grid computing, Mobility, Cloud etc…
  - Identity and Data security becomes evolving perimeters
  - “Trust” is really hard… I even did “academic surgery” and descoped it in my magnum opus ☺
- The skills gap
  - ≈ 200 000 jobs in the USA with similar numbers in other markets
  - How will this be addressed as an industry and what could my part be ?

AFTER THE CONFERENCE

MY THINKING AFTER I WENT…

- Product offerings are moving from “bolt on” to “baked in” security
  - Microsoft: IoT with secure microprocessors (Azure Sphere)
  - Google: Cloud Platform with security functionality : (DLP), traffic segmentation etc
  - Centralized policy management tools seems to still be a bit of a gap as I observed
  - API products vs API Security products: the focus of engineering both products was very clear and the recurring theme of security after the fact emerged…
- Managed security services
  - Definitely a feasible offering to address the skills gap, ROI is really shaped for the organizations with some serious money
  - The Gap that I perceived was the servicing of smaller entities with smaller budgets: Your Doctor, Lawyer etc…

MY THINKING AFTER I WENT…

- Machine Learning has permeated every topic and 90% of the products
  - Everyone that has analytics, has machine learning…the “souped up” version…like a GTI in Durban
  - It was hard to verify, it seemed that it was fairly basic , and my views were supported by a lack of:
    - Classification Accuracy (1)
    - Logarithmic Loss (2)
    - Confusion Matrix (3)
    - Area under Curve (4)
    - F1 Score (5)
    - Mean Absolute Error (6) and Mean Squared Error (7)

1 $$Accuracy = \frac{Number\ of\ Correct\ predictions}{Total\ number\ of\ predictions\ made}$$

2 $$LogarithmicLoss = \frac{-1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M} y_{ij} * \log(p_{ij})$$

3

n=165	Predicted: NO	Predicted: YES
Actual: NO	50	10
Actual: YES	5	100

3 $$Accuracy = \frac{TruePositives + FalseNegatives}{TotalNumberofSamples}$$

4 $$TruePositiveRate = \frac{TruePositive}{FalseNegative + TruePositive}$$

4 $$FalsePositiveRate = \frac{FalsePositive}{FalsePositive + TrueNegative}$$

5 $$F1 = 2 * \frac{1}{\frac{1}{precision} + \frac{1}{recall}}$$

6 $$MeanAbsoluteError = \frac{1}{N}\sum_{j=1}^{N}|y_j - \hat{y}_j|$$

7 $$MeanSquaredError = \frac{1}{N}\sum_{j=1}^{N}(y_j - \hat{y}_j)^2$$

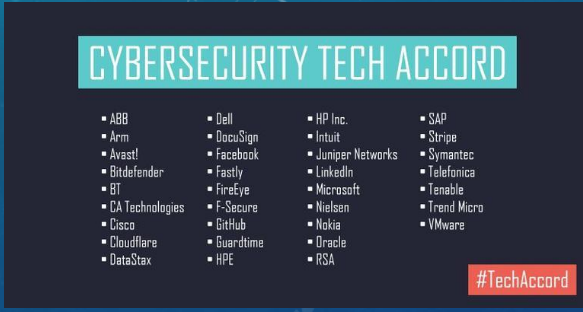
VECTRA
Security that thinks.

Bay Dynamics

LogRhythm
The Security Intelligence Company

MY THINKING AFTER I WENT…

- The building of the Cybersecurity community
  - Looking at the speakers, session leaders etc…they can definitely do with a dose of heterogeneity…it was very US centric while the attendees came from all parts of the globe
  - Moving forward…there is a tech sector accord intended to protect all users, oppose all attacks, empower users and establish a working relationship for vendors across the tech industry



CYBERSECURITY TECH ACCORD

- ABB
- Arm
- Avast!
- Bitdefender
- BT
- CA Technologies
- Cisco
- Cloudflare
- DataStax
- Dell
- DocuSign
- Facebook
- Fastly
- FireEye
- F-Secure
- GitHub
- Guardtime
- HPE
- HP Inc.
- Intuit
- Juniper Networks
- LinkedIn
- Microsoft
- Nielsen
- Nokia
- Oracle
- RSA
- SAP
- Stripe
- Symantec
- Telefonica
- Tenable
- Trend Micro
- VMware

#TechAccord

- Platforms …
  - Product convergence: Cisco, FireEye, McAfee, Symantec are busy with integrating each of their point solutions with 3rd party vendors to create their converged platforms. Obviously, the transition is a concern for us as clients and we should be looking for assurances as they transition…with our current product sets and related product development
- The holy grail …. Holistic Risk Management
  - Cybersecurity and business risk overlap and there is a greater need for solutions that report on focal items such as: application security, assets, configuration management, vulnerability management, 3rd party risk management across the whole enterprise roti roll…

KEYNOTES

BEST KEYNOTE

- The price of Cyber-Warfare
  - Humans feel the pain
  - Historically, we didn’t show the human impact really well
  - As professionals, collaboration with transparency results in very few safe havens for criminals
  - https://www.rsaconference.com/videos/the-price-of-cyber-warfare

BEST KEYNOTE

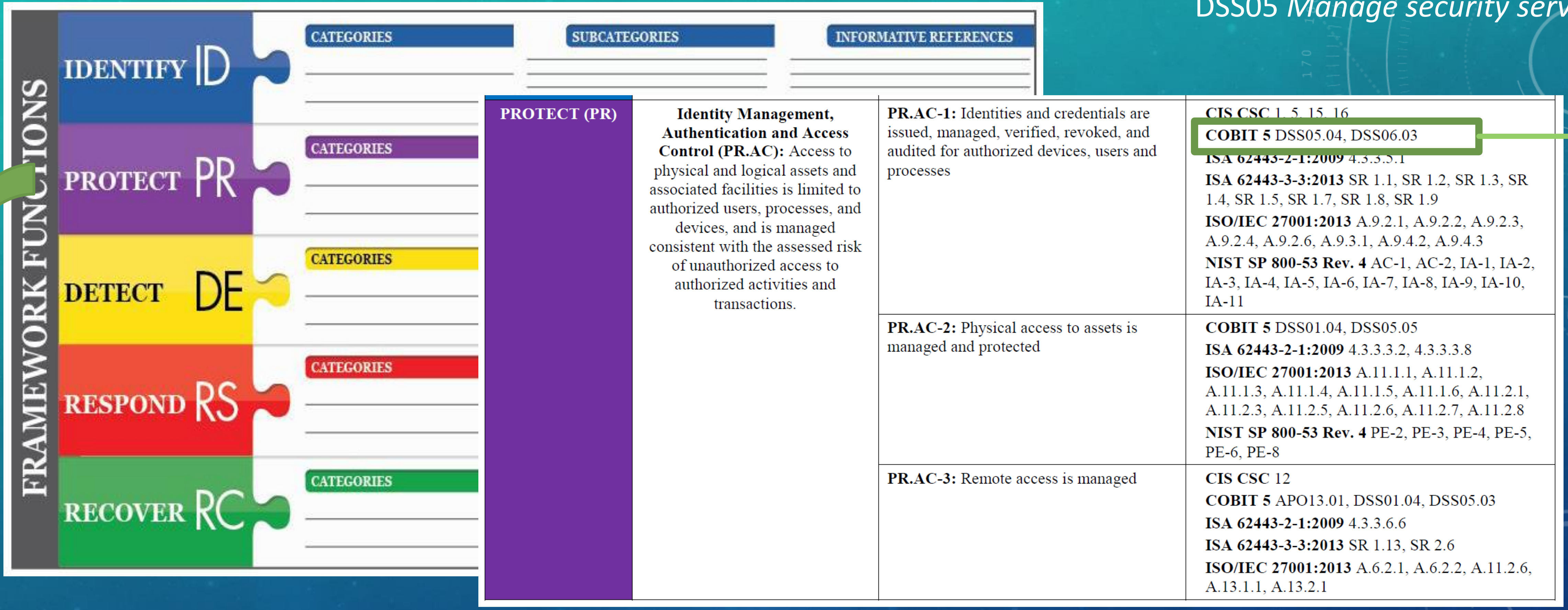
3.55-6.16

8.00-10.40

SESSIONS

NIST CYBERSECURITY FRAMEWORK V 1.1

DSS05 *Manage security services*



PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

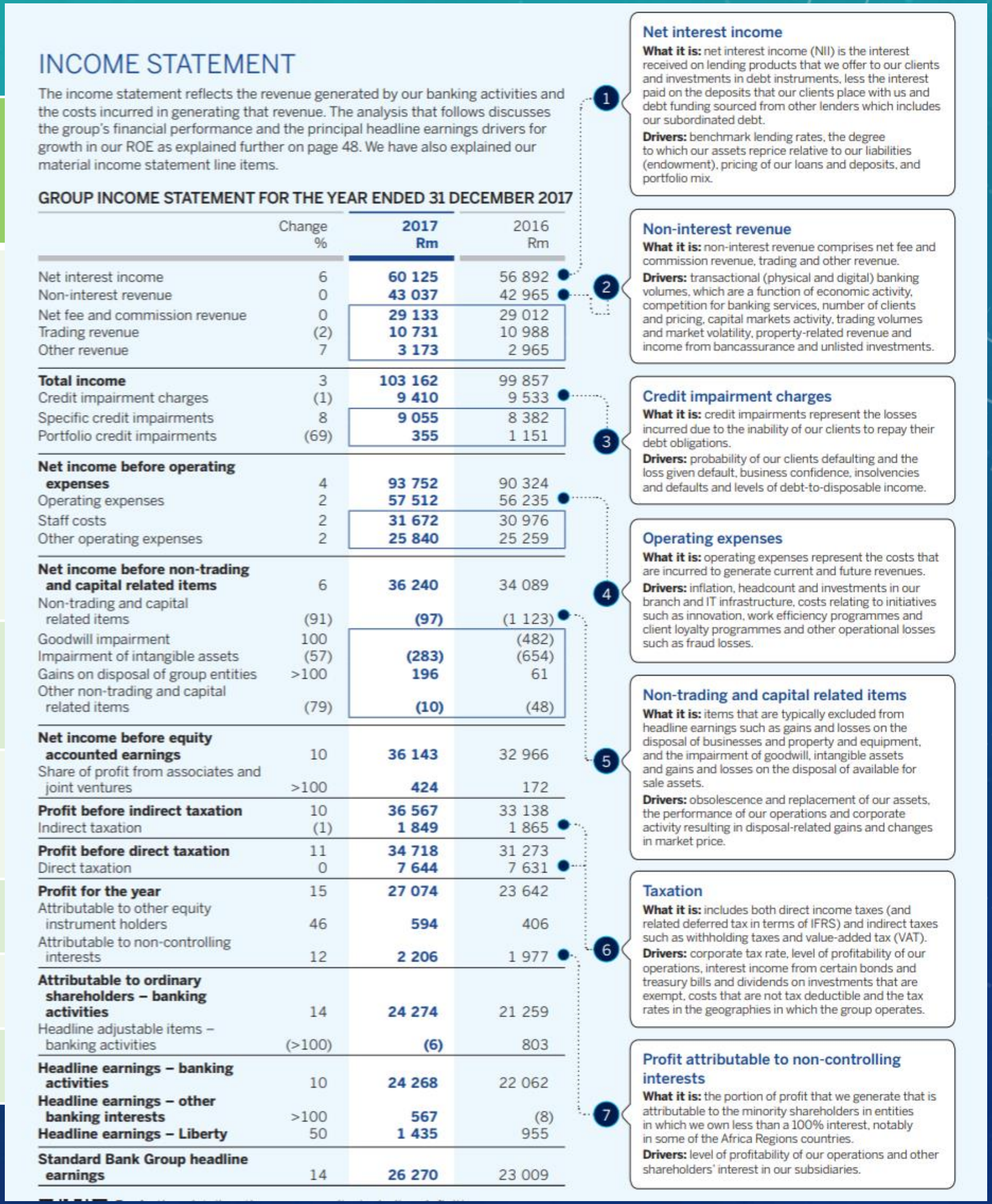
Develop and implement appropriate safeguards to ensure delivery of critical services.

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

End-point security (antivirus/antimalware software, web/email security, firewalls) should be deployed and managed to ensure that laptops, desktops, servers and mobile devices are adequately secured (as measured against value of information). High-value targets (e.g., crown jewels) should be protected with stronger security and controls

HOW TO BEAT MBAs AT THEIR OWN GAME ON A PAGE

Understand Public Market Dynamics	Stock market
	Who owns us
	Role of Analysts
Understanding Roles	CEO/Board
	Growth and Margins
	Peers
Understanding the Financial Statement	
Understand Communication	Do you have an agenda ?
Align to the strategy	Practice <-> Strategy



INCOME STATEMENT

The income statement reflects the revenue generated by our banking activities and the costs incurred in generating that revenue. The analysis that follows discusses the group's financial performance and the principal headline earnings drivers for growth in our ROE as explained further on page 48. We have also explained our material income statement line items.

GROUP INCOME STATEMENT FOR THE YEAR ENDED 31 DECEMBER 2017

	Change %	2017 Rm	2016 Rm
Net interest income	6	**60 125**	56 892
Non-interest revenue	0	**43 037**	42 965
Net fee and commission revenue	0	**29 133**	29 012
Trading revenue	(2)	**10 731**	10 988
Other revenue	7	**3 173**	2 965
Total income	3	**103 162**	99 857
Credit impairment charges	(1)	**9 410**	9 533
Specific credit impairments	8	**9 055**	8 382
Portfolio credit impairments	(69)	**355**	1 151
Net income before operating expenses	4	**93 752**	90 324
Operating expenses	2	**57 512**	56 235
Staff costs	2	**31 672**	30 976
Other operating expenses	2	**25 840**	25 259
Net income before non-trading and capital related items	6	**36 240**	34 089
Non-trading and capital related items	(91)	**(97)**	(1 123)
Goodwill impairment	100		(482)
Impairment of intangible assets	(57)	**(283)**	(654)
Gains on disposal of group entities	>100	**196**	61
Other non-trading and capital related items	(79)	**(10)**	(48)
Net income before equity accounted earnings	10	**36 143**	32 966
Share of profit from associates and joint ventures	>100	**424**	172
Profit before indirect taxation	10	**36 567**	33 138
Indirect taxation	(1)	**1 849**	1 865
Profit before direct taxation	11	**34 718**	31 273
Direct taxation	0	**7 644**	7 631
Profit for the year	15	**27 074**	23 642
Attributable to other equity instrument holders	46	**594**	406
Attributable to non-controlling interests	12	**2 206**	1 977
Attributable to ordinary shareholders – banking activities	14	**24 274**	21 259
Headline adjustable items – banking activities	(>100)	**(6)**	803
Headline earnings – banking activities	10	**24 268**	22 062
Headline earnings – other banking interests	>100	**567**	(8)
Headline earnings – Liberty	50	**1 435**	955
Standard Bank Group headline earnings	14	**26 270**	23 009

1

Net interest income

What it is: net interest income (NII) is the interest received on lending products that we offer to our clients and investments in debt instruments, less the interest paid on the deposits that our clients place with us and debt funding sourced from other lenders which includes our subordinated debt.

Drivers: benchmark lending rates, the degree to which our assets reprice relative to our liabilities (endowment), pricing of our loans and deposits, and portfolio mix.

2

Non-interest revenue

What it is: non-interest revenue comprises net fee and commission revenue, trading and other revenue.

Drivers: transactional (physical and digital) banking volumes, which are a function of economic activity, competition for banking services, number of clients and pricing, capital markets activity, trading volumes and market volatility, property-related revenue and income from bancassurance and unlisted investments.

3

Credit impairment charges

What it is: credit impairments represent the losses incurred due to the inability of our clients to repay their debt obligations.

Drivers: probability of our clients defaulting and the loss given default, business confidence, insolvencies and defaults and levels of debt-to-disposable income.

4

Operating expenses

What it is: operating expenses represent the costs that are incurred to generate current and future revenues.

Drivers: inflation, headcount and investments in our branch and IT infrastructure, costs relating to initiatives such as innovation, work efficiency programmes and client loyalty programmes and other operational losses such as fraud losses.

5

Non-trading and capital related items

What it is: items that are typically excluded from headline earnings such as gains and losses on the disposal of businesses and property and equipment, and the impairment of goodwill, intangible assets and gains and losses on the disposal of available for sale assets.

Drivers: obsolescence and replacement of our assets, the performance of our operations and corporate activity resulting in disposal-related gains and changes in market price.

6

Taxation

What it is: includes both direct income taxes (and related deferred tax in terms of IFRS) and indirect taxes such as withholding taxes and value-added tax (VAT).

Drivers: corporate tax rate, level of profitability of our operations, interest income from certain bonds and treasury bills and dividends on investments that are exempt, costs that are not tax deductible and the tax rates in the geographies in which the group operates.

7

Profit attributable to non-controlling interests

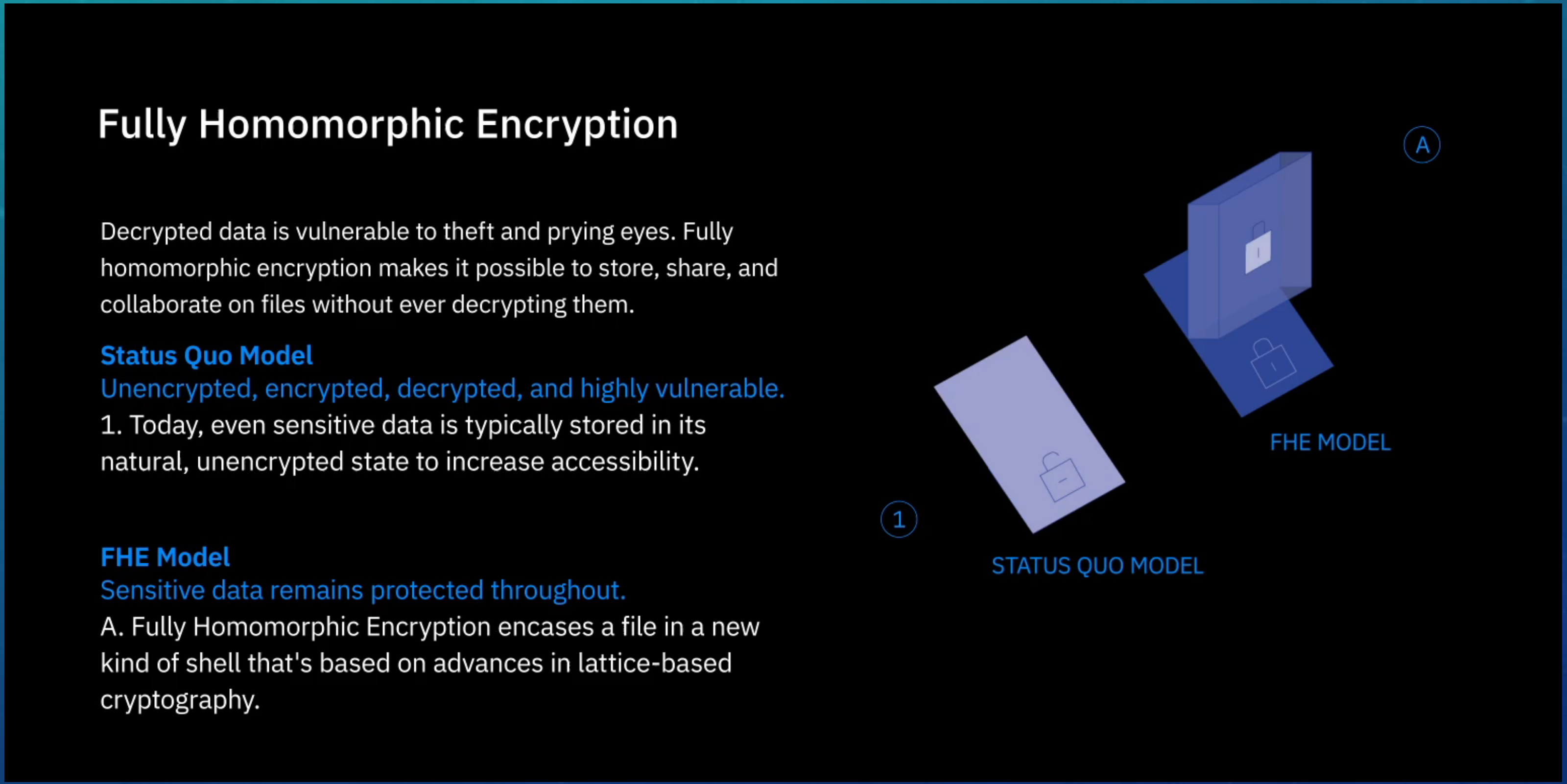
What it is: the portion of profit that we generate that is attributable to the minority shareholders in entities in which we own less than a 100% interest, notably in some of the Africa Regions countries.

Drivers: level of profitability of our operations and other shareholders' interest in our subsidiaries.

1. Over 50% of SBG shares are owned by foreigners…

HOMOMORPHIC ENCRYPTION ON A PAGE

- A system in which computations performed on ciphertext produce identical results to those carried out on plaintext, has been known in theory since 1978 and technically feasible since at least 2009.
- This means that you can keep data encrypted as you query, process, and analyze it.
- For example, a retailer could encrypt a customer's credit card number at first use and keep it to use for future transactions without fear, because they'd never need to decrypt it.
- So why isn't everyone already doing this? Because, until recently, it was far too slow for commercial use. However, researchers then managed to reduce the processing time.
- Very much in infancy : https://www.theregister.co.uk/2018/03/08/ibm_faster_homomorphic_encryption/



Fully Homomorphic Encryption

Decrypted data is vulnerable to theft and prying eyes. Fully homomorphic encryption makes it possible to store, share, and collaborate on files without ever decrypting them.

Status Quo Model
Unencrypted, encrypted, decrypted, and highly vulnerable.
1. Today, even sensitive data is typically stored in its natural, unencrypted state to increase accessibility.

FHE Model
Sensitive data remains protected throughout.
A. Fully Homomorphic Encryption encases a file in a new kind of shell that's based on advances in lattice-based cryptography.

PRODUCTS

SOME KEY PRODUCTS

BayDynamics

- Product Name: Risk Fabric
- Key Features:
  - Cyber risk analytics platform that calculates the value at risk associated with specific threats and vulnerabilities, and prescribes actions to measurably reduce cyber risk exposure.
  - Using patented contextual data models and user and entity behavioral analytics (UEBA) technologies, stakeholders across the business common can now have metrics that prioritize remediation activities to the risks that matter most

BayDynamics

BEYOND SECURITY

- Product Name: beSOURCE
- Key Features:
  - Static Application Security Testing tool that aims to educate developers about the problems it finds.
  - Has a compiler-free inspection engine and works with several programming languages. Currently a stand alone tool for individual developers.

BEYOND SECURITY

GUARDICORE

- Product Name: Centra Security Platform
- Key Features:
  - Containerized workload protection for the data centre.
  - IT security teams can have visibility of every container, pod and service, visualize their communication flows and secure them with micro-segmentation policies.
  - Also detection of threats within individual containers and quarantine them.

GUARDICORE

Process Visibility with Docker Containers

GuardiCore

Securing the Software Defined Data Center

F5 Networks

- Product Name: DDos Hybrid Defender
- Key Features:
  - Combination of on-premise appliance coupled with a cloud-based scrubbing service that can handle the overflow from very large attacks.
  - Appliance works at the network and application layers, spotting application-level attacks that are hurting performance and developing custom mitigation signatures automatically.

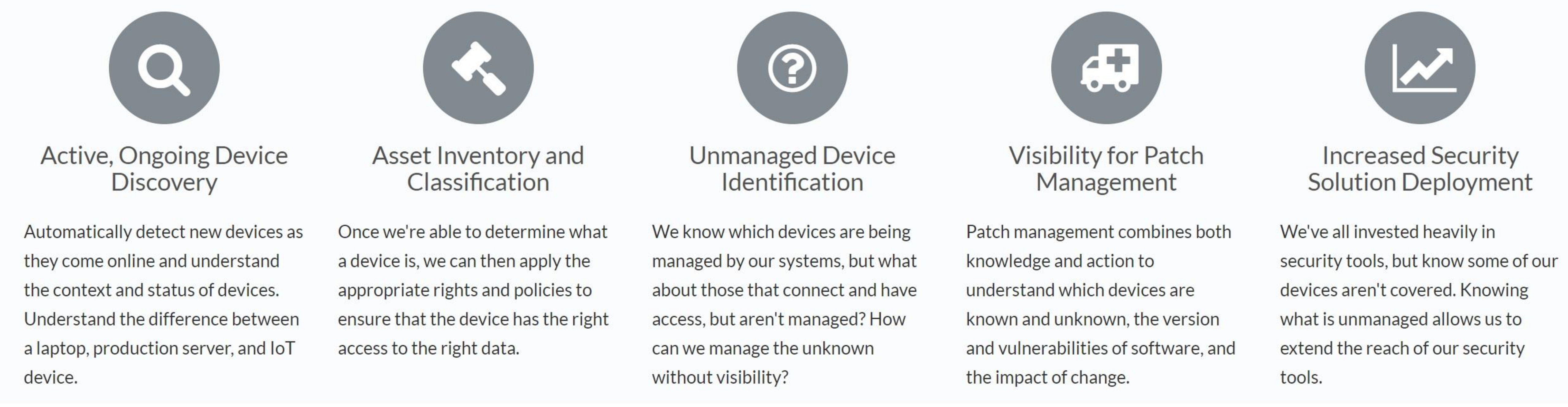
F5 Netowrks

F5 DDoS Hybrid Defender
Automated Blocking of Layer 7 DoS

f5
WE MAKE APPS GO
FASTER.
SMARTER.
SAFER.

AXONIUS

- Product name: Cybersecurity Asset Management Platform
- Key Features:
  - Comprehensive view of all devices on your network using extensible plugin system to gather data from security and management tools you already have, inclusive of :
    - Identity and Auth. Systems, Network Access Control (NAC), Firewalls, Vulnerability Scanners, Switches, Security Information & Event Management Endpoint Detection & Response etc…
- https://www.axonius.com/unified-device-management/



Active, Ongoing Device Discovery

Automatically detect new devices as they come online and understand the context and status of devices. Understand the difference between a laptop, production server, and IoT device.

Asset Inventory and Classification

Once we're able to determine what a device is, we can then apply the appropriate rights and policies to ensure that the device has the right access to the right data.

Unmanaged Device Identification

We know which devices are being managed by our systems, but what about those that connect and have access, but aren't managed? How can we manage the unknown without visibility?

Visibility for Patch Management

Patch management combines both knowledge and action to understand which devices are known and unknown, the version and vulnerabilities of software, and the impact of change.

Increased Security Solution Deployment

We've all invested heavily in security tools, but know some of our devices aren't covered. Knowing what is unmanaged allows us to extend the reach of our security tools.

FIREMON

- Product Name: FireMon Global Policy Controller
- Key Features: Enforces global policy by automatically performing compliance checks before applications or asserts are pushed onto the network. Business intent into specific security rules, giving “self-service” to DevOps and other application owners.

- Policy Compute Engine, which provides the following capabilities:
  - **Dynamic policy change**: Instantly adapting to network changes, FireMon GPC creates a continuous state of security across all IT assets in any environment, at all times.
  - **Embedded security**: Before any applications or assets are pushed onto the network, FireMon GPC automatically performs a compliance check to ensure the right policies are assigned. By enforcing policy “guardrails,” FireMon GPC ensures continuous security on a global scale.
  - **Intent translation**: FireMon GPC automatically translates business intent into specific security rules, with no human intervention. This enables new applications to deploy in seconds rather than hours or even days, while eliminating human error.
  - **Automated distribution**: By automatically distributing the right rules to any enforcement point, FireMon GPC provides DevOps and other application owners with guided “self-serve” security capabilities. This eliminates the delays caused by traditional manual rules creation and provisioning.