CYBERSECURITY FOR INSURANCE SERVICE PROVIDERS

Raymond Bett

19th Jun 2018

www.stractconsult.com +254 727 683 641

Who am I?

Name: Raymond Bett
Competency: System Audits, IT security testing/Penetration testing, Cybersecurity risk assessment, Quality Assurance, Data Analytics

Educational Qualifications

- BSc Electrical and Information Engineering, University of Nairobi

Certifications

- Certified Information Systems Auditor (CISA)
- Certified information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Ethical Hacker (CEH)
- Cybersecurity Fundamentals Certificate
- Certified Public Accountant (CPA-K)

Memberships

- Information Systems Audit and Control
- Association (ISACA) – Vice President of the Kenya Chapter
- Institute of Certified Public Accountants (ICPAK)

Professional Experience

- Stract Consulting, Principal Cybersecurity Consultant (2016-current)
- Safaricom Limited 5 years, Principal Information Systems Auditor (2012-2016)
- PricewaterhouseCoopers (PwC) 2 years, Systems and Process Assurance (2010 – 2012)

Profile Brief

Raymond Bett is an experienced information security auditor. He has over 9 years experience in carrying out risk based review of IT environments in some of the most complex organizations with large ICT systems. The systems he has reviewed ranged from Mobile money payment systems, core banking systems, enterprise resource planning systems such as Oracle, Microsoft Dynamics Nav and SAP.

Technology Capabilities

- Information Systems audits.
- IT risk assessment;
- System security reviews through penetration testing and vulnerability assessments;
- Enterprise Resource Planning (ERP) reviews;
- Review of application controls, database controls (SQL) and Operating system server controls;
- Quality Assurance over system implementations.
- Project Management;

Methodology:

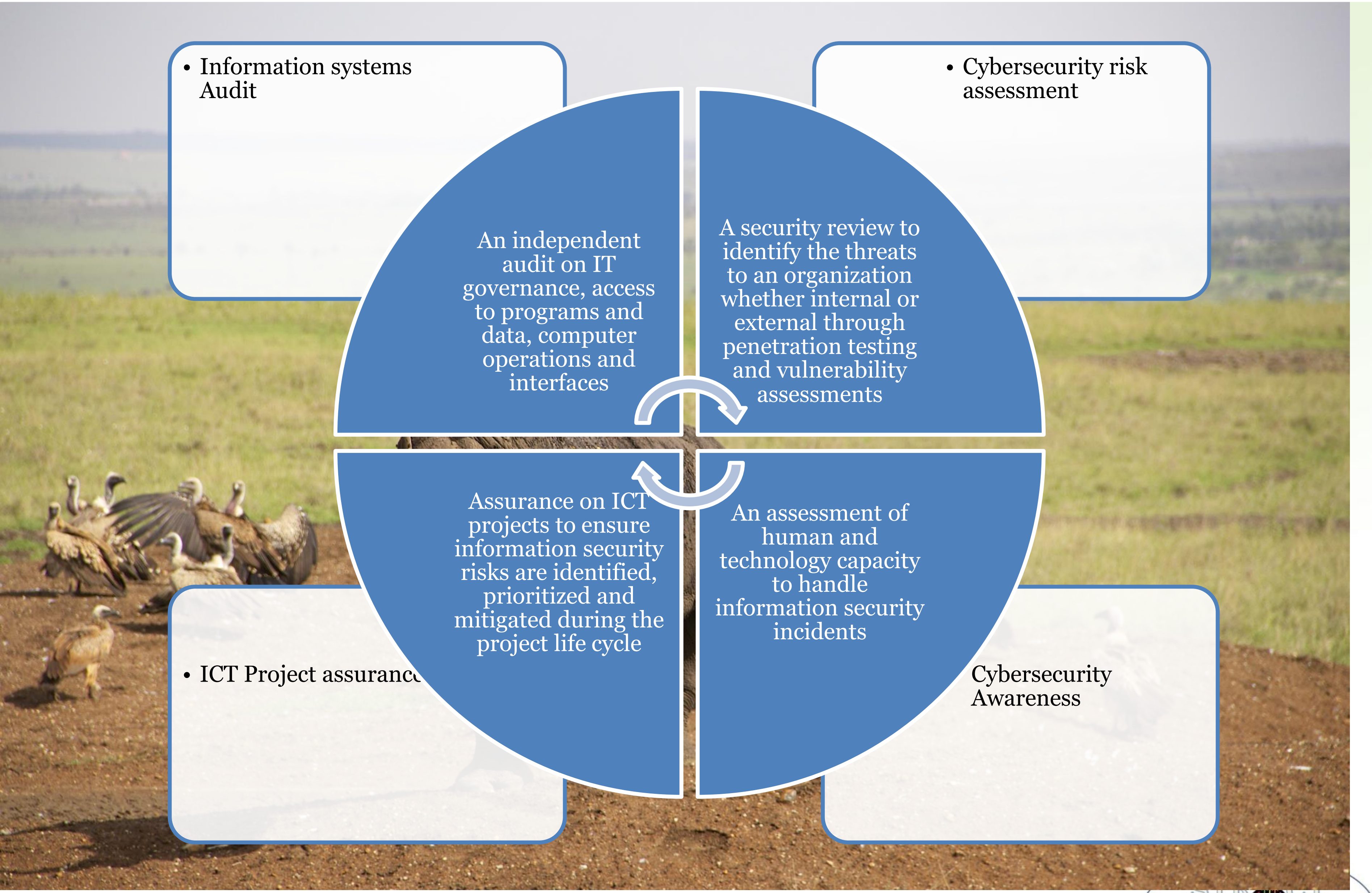
- ISO 27001
- Institute of Internal Audit (IIA) Methodology
- ISACA Methodology
- Stract Consulting Proprietary Methodology
- COBIT Methodology

STRACT CONSULTING
Equipped to deliver

ABOUT STRACT CONSULTING COMPANY

Stract Consulting is a professional service firm, that provides cybersecurity consultancy services in the areas of information systems audit, information technology consulting, information technology project assurance and information technology risk management consulting . We have a team of qualified and experience professionals in this area and we provide a guaranteed best in class service.

Stract Consulting Service Offering



- Information systems Audit

An independent audit on IT governance, access to programs and data, computer operations and interfaces

- Cybersecurity risk assessment

A security review to identify the threats to an organization whether internal or external through penetration testing and vulnerability assessments

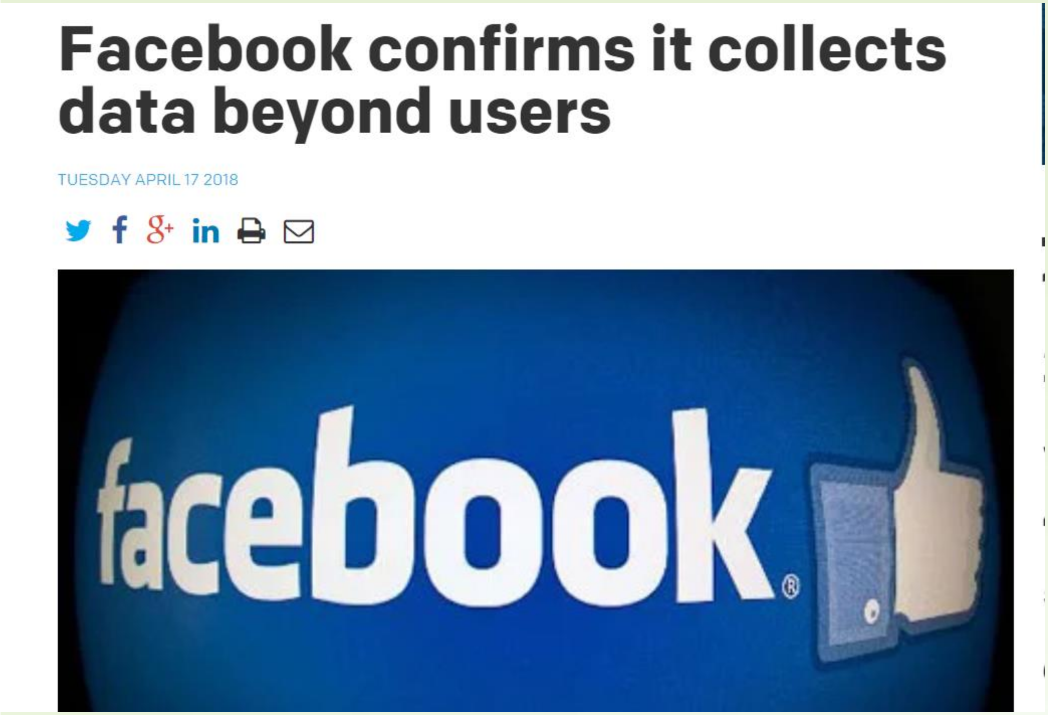
- ICT Project assurance

Assurance on ICT projects to ensure information security risks are identified, prioritized and mitigated during the project life cycle

Cybersecurity Awareness

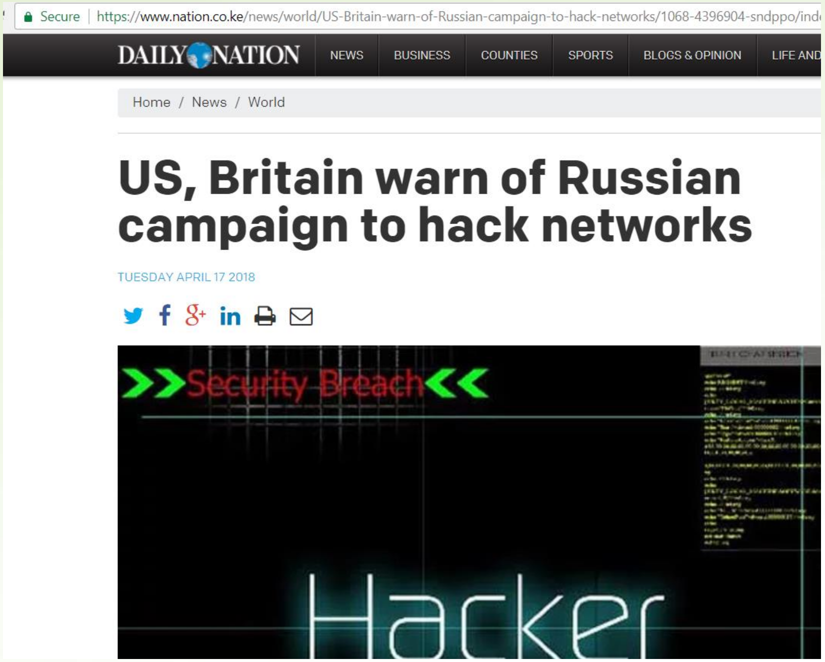
An assessment of human and technology capacity to handle information security incidents

CYBER ATTACKS IN THE HEADLINES



Facebook confirms it collects data beyond users

TUESDAY APRIL 17 2018

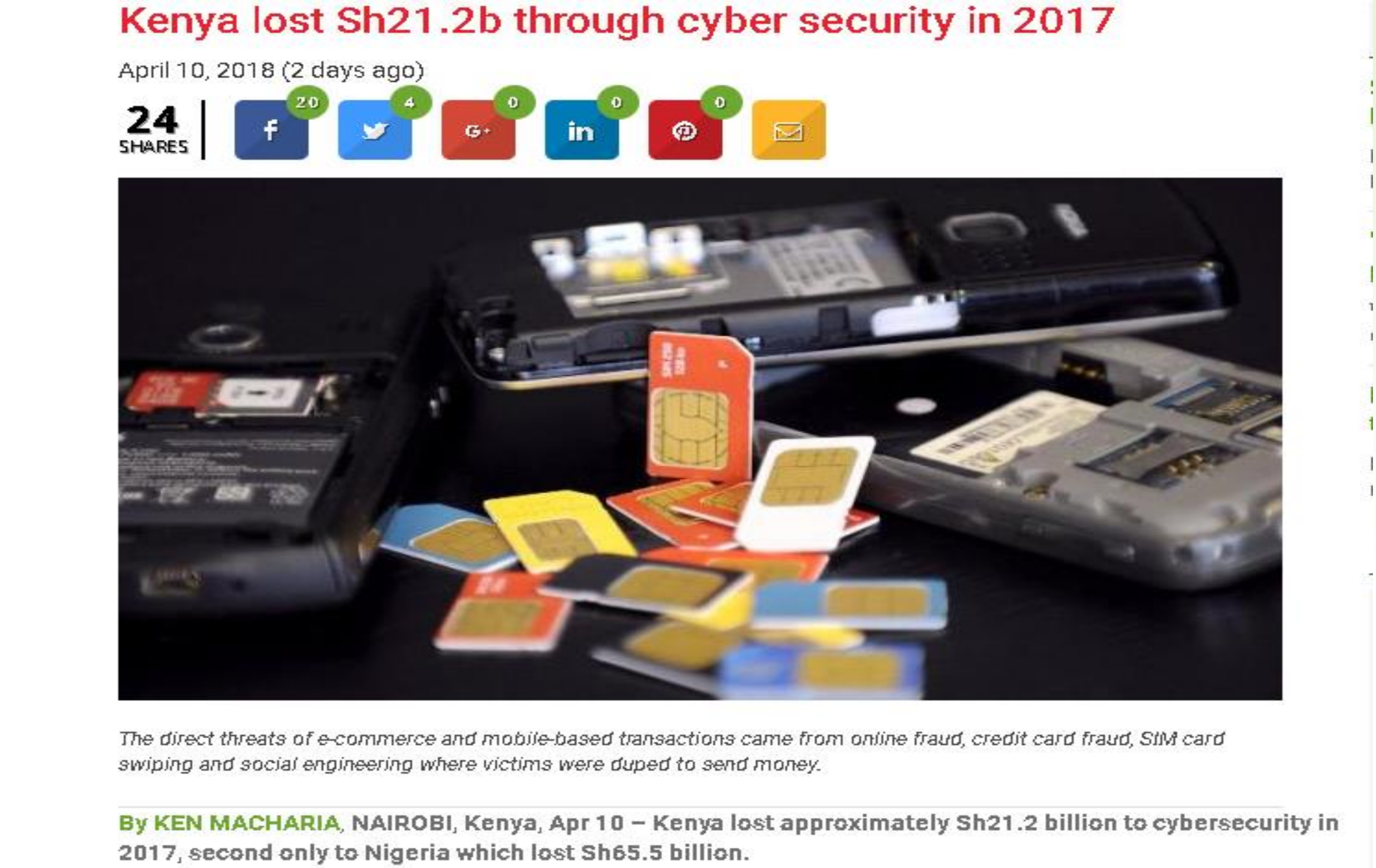


Secure | https://www.nation.co.ke/news/world/US-Britain-warn-of-Russian-campaign-to-hack-networks/1068-4396904-sndppo/ind

US, Britain warn of Russian campaign to hack networks

TUESDAY APRIL 17 2018

THE HEADLINES



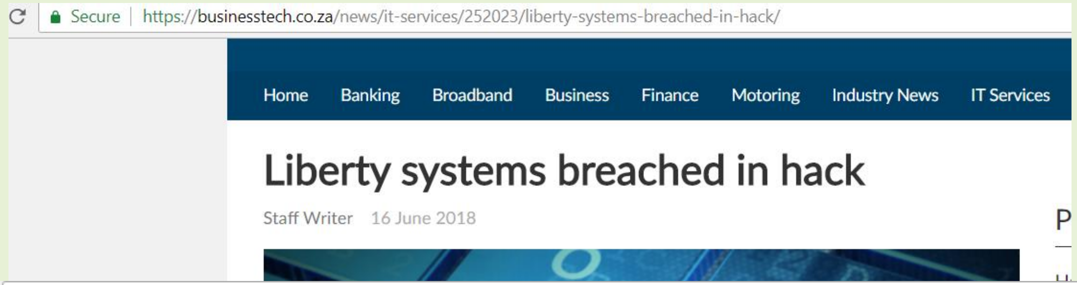
Kenya lost Sh21.2b through cyber security in 2017

April 10, 2018 (2 days ago)

The direct threats of e-commerce and mobile-based transactions came from online fraud, credit card fraud, SIM card swiping and social engineering where victims were duped to send money.

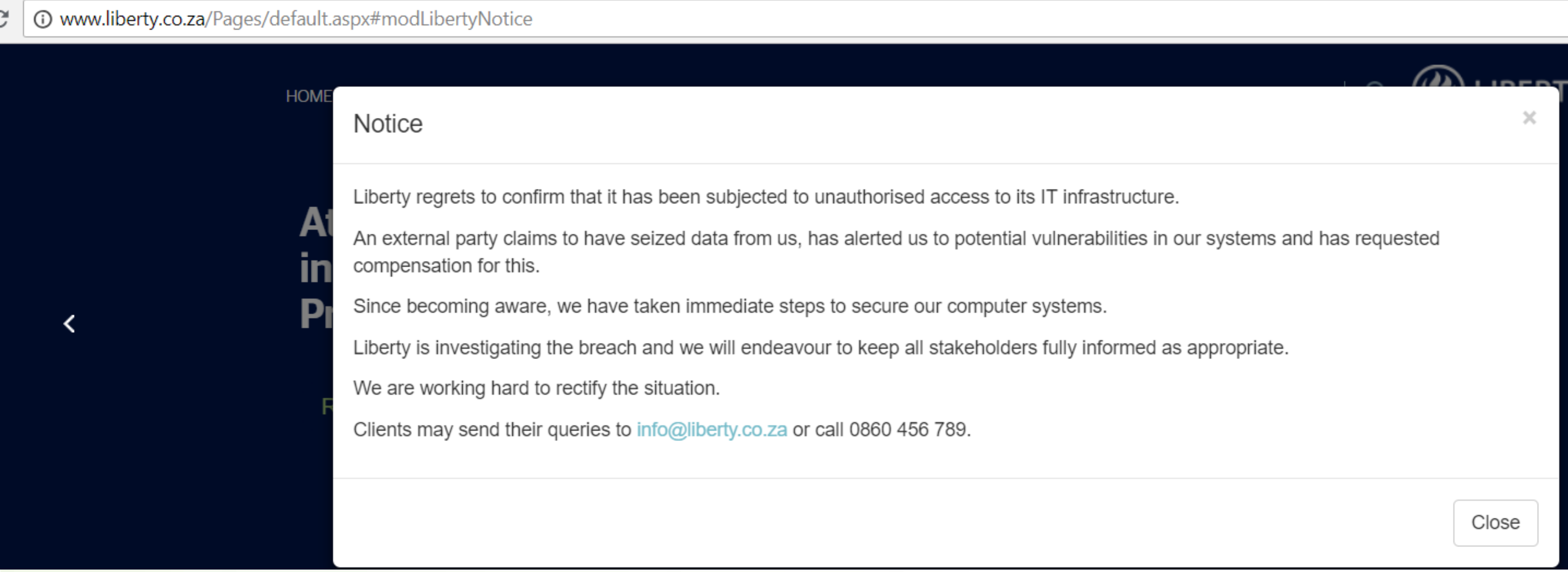
By KEN MACHARIA, NAIROBI, Kenya, Apr 10 – Kenya lost approximately Sh21.2 billion to cybersecurity in 2017, second only to Nigeria which lost Sh65.5 billion.

CYBER ATTACKS IN THE HEADLINES


Secure
https://businesstech.co.za/news/it-services/252023/liberty-systems-breached-in-hack/
Home
Banking
Broadband
Business
Finance
Motoring
Industry News
IT Services

Liberty systems breached in hack

Staff Writer 16 June 2018



Notice

Liberty regrets to confirm that it has been subjected to unauthorised access to its IT infrastructure.

An external party claims to have seized data from us, has alerted us to potential vulnerabilities in our systems and has requested compensation for this.

Since becoming aware, we have taken immediate steps to secure our computer systems.

Liberty is investigating the breach and we will endeavour to keep all stakeholders fully informed as appropriate.

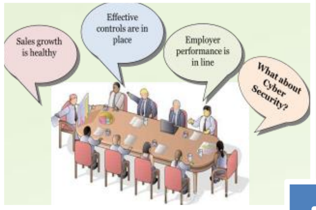
We are working hard to rectify the situation.

Clients may send their queries to info@liberty.co.za or call 0860 456 789.

CYBERSECURITY STATISTICS

KSh 21 Billion, the cost of Cybercrime in Kenya in 2017 as per Serianu Report

40 Million, the number of Internet users in Kenya – Communications Authority


Sales growth is healthy
Effective controls are in place
Employer performance is in line
What about Cyber Security?

60% of CEOs in Africa believe that data breaches will impact stakeholder trust – PwC Africa business Agenda

20% of Kenyan users are attacked by Mobile Malware – Kaspersky

COMPUTER MISUSE AND CYBERCRIME ACT, 2018

The Computer Misuse and Cybercrimes Act was assented to by President Uhuru Kenyatta on 16th May 2018. The High Court has temporarily suspended 26 sections of the Cyber crime law.

Offense	Fine	Imprisonment term
Unauthorized access	5 Million	3 years
Unauthorized interference	10 Million	5 years
Unauthorized interception	10 Million	5 years
Illegal devices and access codes	20 Million	10 years
Unauthorised disclosure of password or access code	5 Million	3 years
Cyber espionage	10 Million	20 years
False publications (“fake News”)	5 Million	2 years
Child pornography	20 Million	25 years
Computer forgery	10 Million	5 years
Computer fraud	20 million	10 years
Cyberstalking, Cyber bullying	20 million	10 years
Cybersquatting	200,000	2 years

CONSULTING

Equipped to deliver

Central Bank of Kenya Guidance Note on Cybersecurity

Professionals

- Need to engage professional with sufficient cybersecurity expertise
- There are **1,600*** certified security professionals, (CISA,CISM, CEH, ISO 27001, PCI DSS) to cover the 43 banks

Frequency of the test

- Need for an independent cyber threat analysis at least once every year annually

Role of Internal auditors

- Need to have internal auditors with sufficient ICT skills and if this cannot be within the organization, they can be outsourced.

Role of risk management function

- Should manage cybersecurity risks within the enterprise risk management portfolio

Role of external auditors

- In addition to the IT audit scope of IT General Controls there is a requirement to carry out a comprehensive penetration tests and report this to CBK

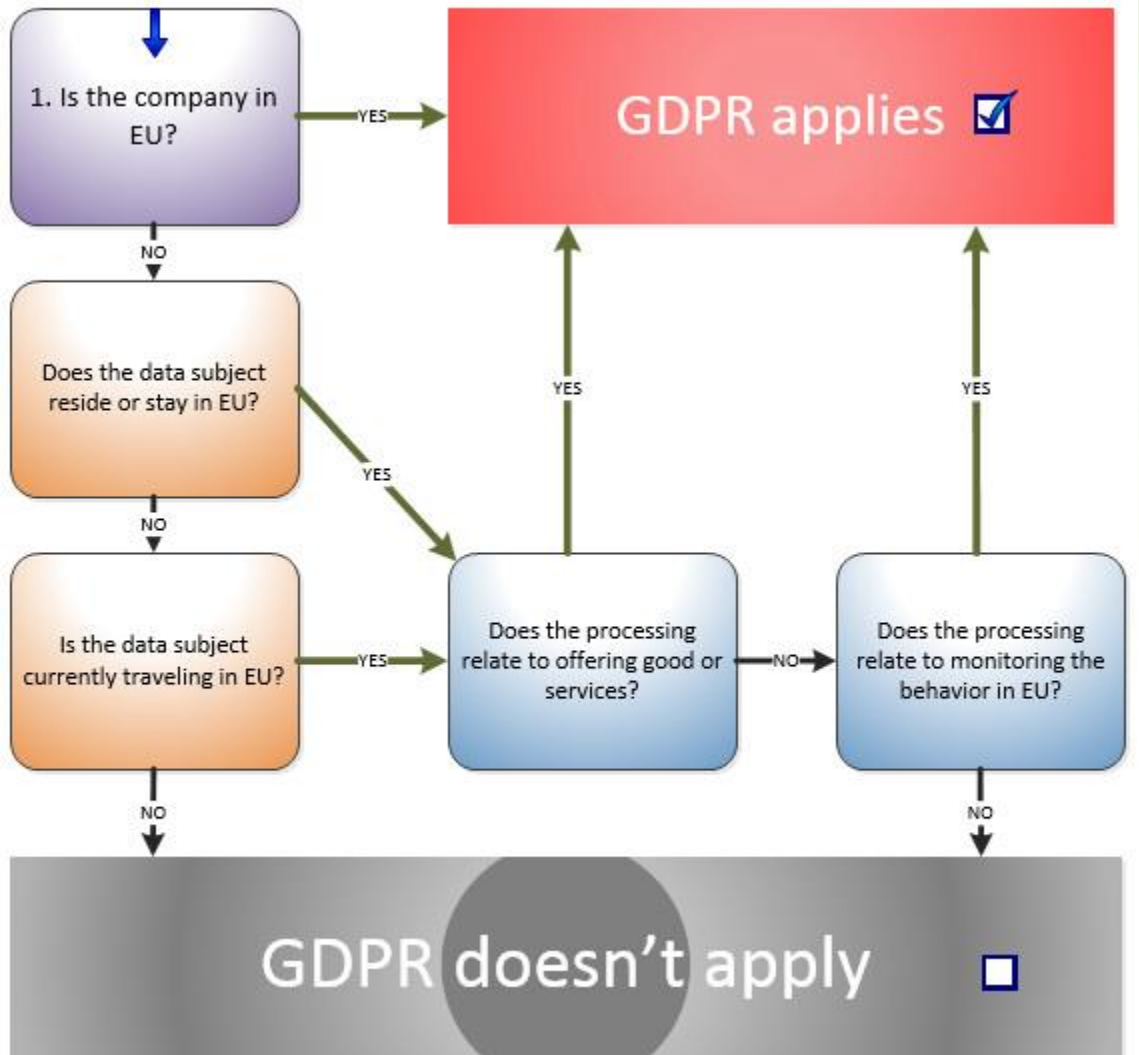
Central Bank of Kenya Guidance Note on Cybersecurity - Summary

	GOVERNANCE	ASSESSMENTS	AWARENESS
Key Enablers	➢ Allocate an adequate cybersecurity budget ➢ Build a cyber-security benchmark framework ➢ Define roles and responsibilities ➢ A comprehensive cyber incident response plan	➢ Assess design and effectiveness of cyber security framework ➢ Regular independent vulnerability and threat assessments by internal and external auditors ➢ Understand extent of automated controls	➢ Implement cyber security awareness training programmes for customers and vendors ➢ A formalised plan to provide ongoing technical trainings to in house cyber security specialists
Key Deliverables	✓ Cyber strategy and Governance charter ✓ Cyber response plan and benchmark framework ✓ Cyber security budget and controls framework	✓ Internal Audit reports for the Board ✓ External audit reports for Board and CBK ✓ Quarterly reporting of incidents to CBK	✓ Cyber security training calendar and plan ✓ Training literature for Board, Employees, Third parties and Customers

STRACT CONSULTING
Equipped to deliver

General Data Protection Regulations (GDPR)

All enterprises that offer goods or services (regardless if payment is required) within the EU as well as any business that retains or processes information on any EU citizen is subject to GDPR and its data protection requirements. In the global, digitized world of commerce, these EU regulations are sure to impact many businesses outside of the EU's borders.


1. Is the company in EU?
YES
GDPR applies ☑
NO
Does the data subject reside or stay in EU?
YES
YES
YES
NO
Is the data subject currently traveling in EU?
YES
Does the processing relate to offering good or services?
NO
Does the processing relate to monitoring the behavior in EU?
NO
NO
GDPR doesn't apply □

General Data Protection Regulations (GDPR)

Fines have gone up to €20 million or 4% of your worldwide turnover for the last 12 months. Below is the summary of the GDPR regulation

Consent

- Data controllers must keep their terms and conditions simple and easy to read

Breach Notification

- In the event of a data breach, data controllers and processors must notify their customers of any risk within 72 hours

Right to access

- Customers have the right to obtain confirmation of whether their personal data is being processed and how

Right to be forgotten

- Customers can ask for all their data to be deleted.

Data portability

- Individuals have the right to obtain and reuse their personal data for their own purposes by transferring it across different IT environments

Privacy by design

- Data protection from the very beginning of designing software, systems, websites etc.

Data Protection Officers

- Professionally qualified officers must be appointed in public authorities or for organisations with more than 250 employees.

STRACT CONSULTING
Equipped to deliver

Other Legislation - National Cybersecurity Framework

National Cybersecurity Framework

Vision 2030

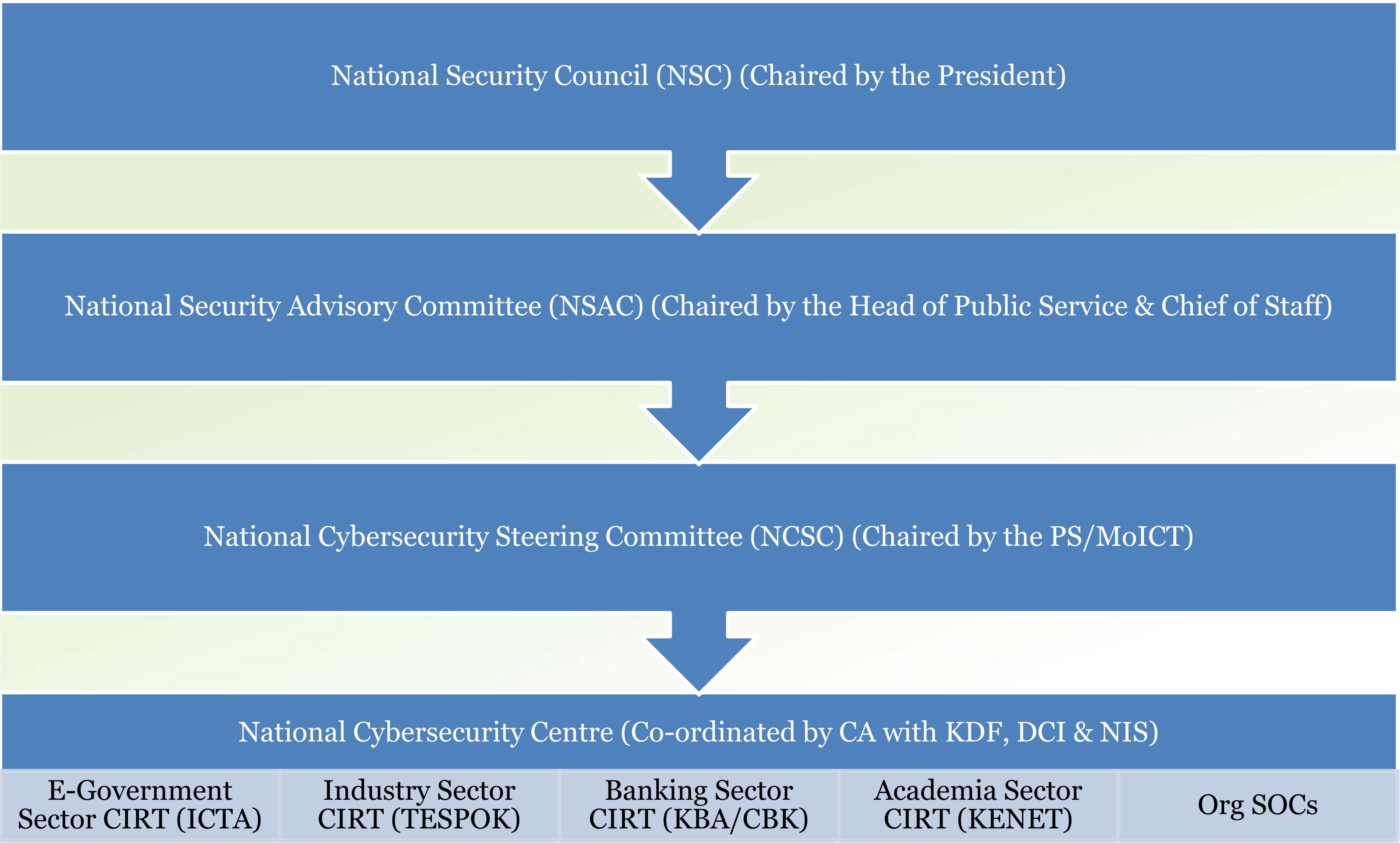
ICT Sector Policy

National Cyber Security Strategy

Kenya Information & Communications Act + Regulations

National KE-CIRT/CC

Other Legislation - National Cybersecurity Framework



National Security Council (NSC) (Chaired by the President)

National Security Advisory Committee (NSAC) (Chaired by the Head of Public Service & Chief of Staff)

National Cybersecurity Steering Committee (NCSC) (Chaired by the PS/MoICT)

National Cybersecurity Centre (Co-ordinated by CA with KDF, DCI & NIS)

E-Government Sector CIRT (ICTA)	Industry Sector CIRT (TESPOK)	Banking Sector CIRT (KBA/CBK)	Academia Sector CIRT (KENET)	Org SOCs

STRACT CONSULTING

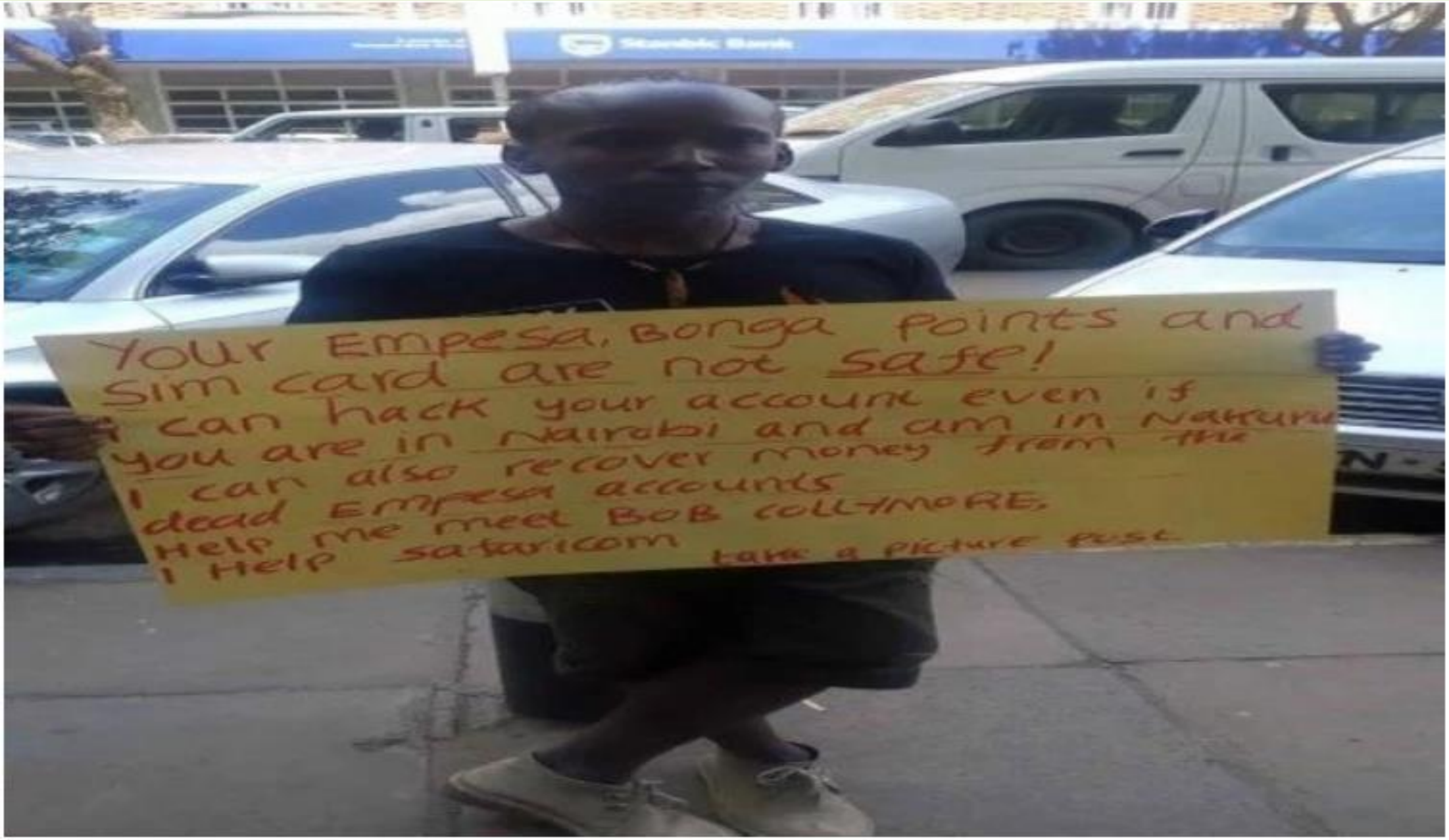
Equipped to deliver

CYBERCRIMINAL

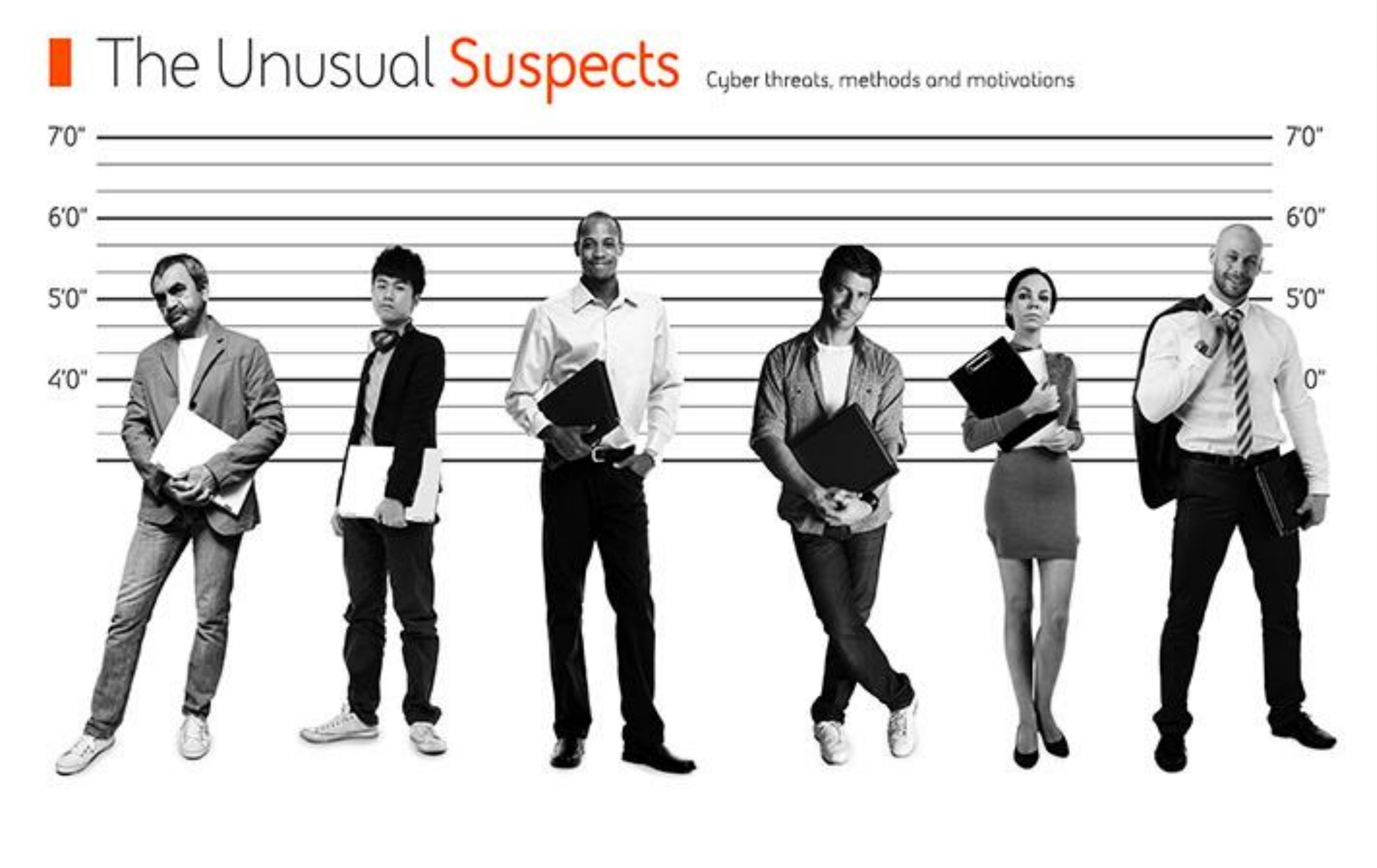
Our imagination of a cybercriminal

CYBERCRIMINAL

Or This


Stanbic Bank
Your Empesa, Bonga points and
Sim card are not safe!
I can hack your account even if
you are in Nairobi and am in Nakuru
I can also recover money from the
dead Empesa accounts
Help me meet BOB COLLYMORE,
I Help safaricom
take a picture post

CYBERCRIMINAL



CYBERCRIMINAL

- They’re too young to go to jail – and know that, even if they’re caught, they’ll get away with little more than a slap on the wrist for their actions.
- Often blessed with merely basic hacking skills, the script kiddie is curious, keen to learn, and also keen to impress peers or more senior cybercriminals. They may not understand the consequences or illegality of their actions.

Script Kiddie

CYBERCRIMINAL

- Whatever their cause, it’s a burning one – and the Activist takes their political, religious or social cause outside the rule of law and on to the Internet. The Activist targets adversaries with data theft, reputational damage and the defacement of web sites and social media accounts E.g. WikiLeaks, local bloggers

Hacktivist

STRACT CONSULTING
Equipped to deliver

CYBERCRIMINAL

- They work at what looks like a legitimate ‘9 to 5’ job – but it’s anything other than law abiding. The Professional has built a career out of committing or supporting cyber crime. They target customers of financial institution through social engineering.

Professional

CYBERCRIMINAL

- They may only be 20% of the threat, but they produce 60% of the damage. These attackers are considered to be the highest risk. To make matters worse, as the name suggests, they often reside within an organization either current employees, former employees, employees of related organizations etc. The threat comes in because the know how the company operates, which are the weak points and so on.

Insiders

CYBERCRIMINAL

- This group is responsible for highly targeted attacks carried out by extremely organized state-sponsored groups. Their technical skills are deep and they have access to vast computing resources. The US election was influenced by Russians who favoured a certain candidate and this was done by hacking the Democratic party systems.

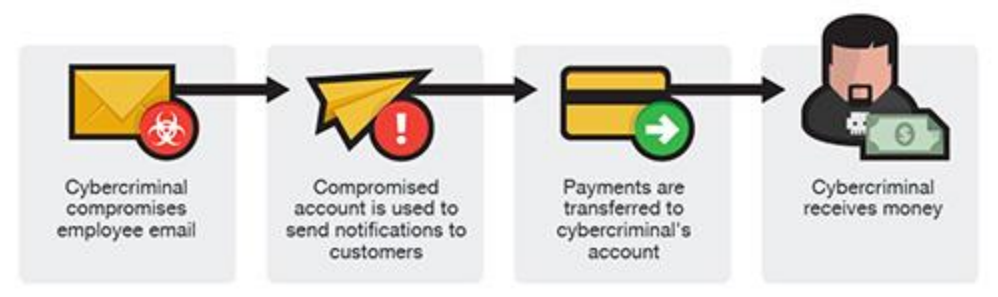
Nation State Actor

STRACT
CONSULTING
Equipped to deliver

INTERNET FRAUD

Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them. Internet crime schemes include:

•**Business E-Mail Compromise (BEC):** A sophisticated scam targeting businesses working with foreign suppliers and companies that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.


Cybercriminal compromises employee email
Compromised account is used to send notifications to customers
Payments are transferred to cybercriminal's account
Cybercriminal receives money

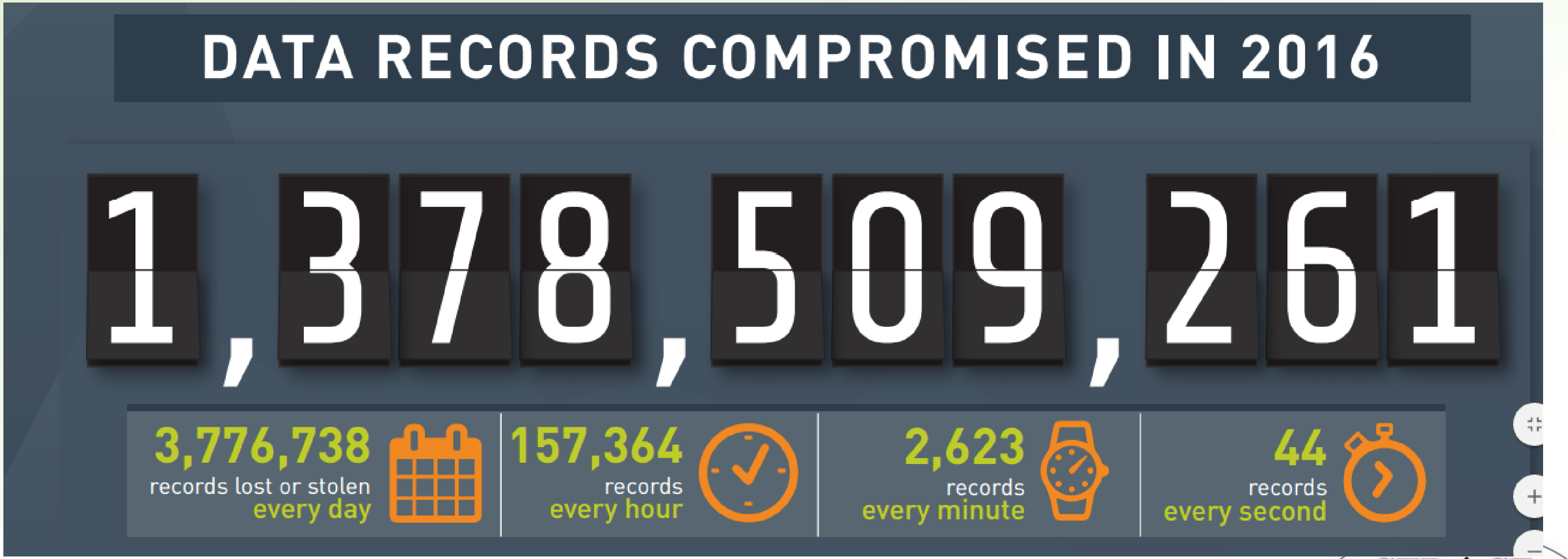
INTERNET FRAUD

- **Fake News** is an inaccurate, sometimes sensationalistic report that is created to gain attention, mislead, deceive or damage a reputation. Unlike misinformation, which is inaccurate because a reporter has confused facts, fake news is created with the intent to manipulate someone or something.

STRACT CONSULTING
Equipped to deliver

INTERNET FRAUD

- **Data Breach:** A leak or spill of data which is released from a secure location to an untrusted environment. Data breaches can occur at the personal and corporate levels and involve sensitive, protected, or confidential information that is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.



DATA RECORDS COMPROMISED IN 2016

1,378,509,261

3,776,738 records lost or stolen every day

157,364 records every hour

2,623 records every minute

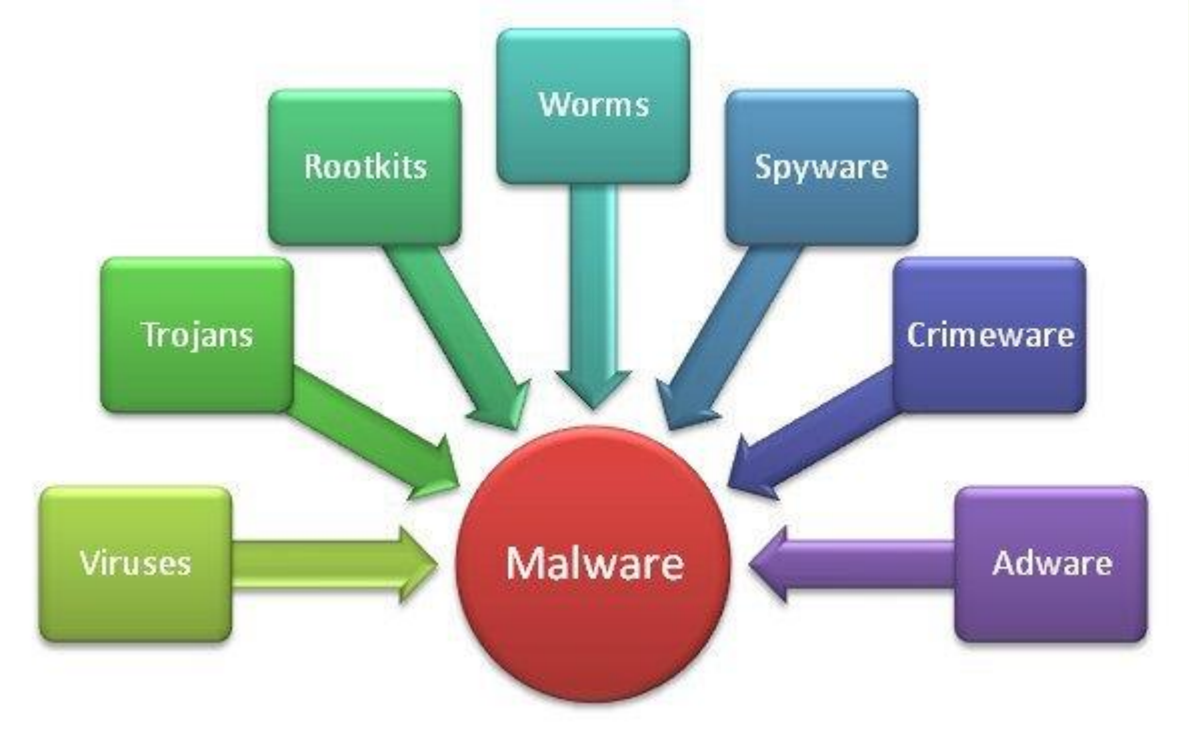
44 records every second

INTERNET FRAUD

- **Denial of Service:** An interruption of an authorized user's access to any system or network, typically one caused with malicious intent.

INTERNET FRAUD

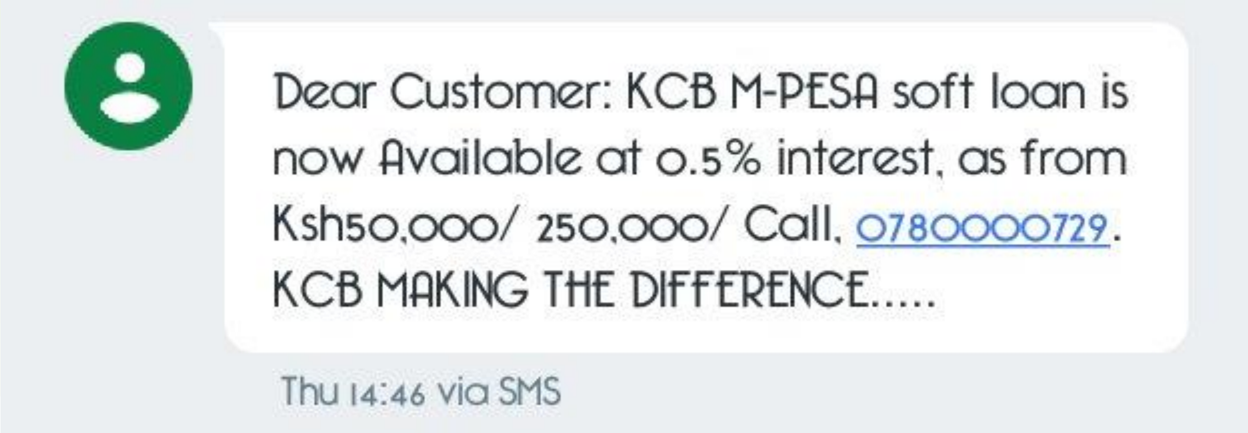
- **Malware/Scareware:** Malicious software that is intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds from victims.



STRACT CONSULTING
Equipped to deliver

INTERNET FRAUD

- **Phishing/Spoofing:** Both terms deal with forged or faked electronic documents. Spoofing generally refers to the dissemination of e-mail which is forged to appear as though it was sent by someone other than the actual source. Phishing is the act of sending an e-mail falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website or asking them to call a certain number

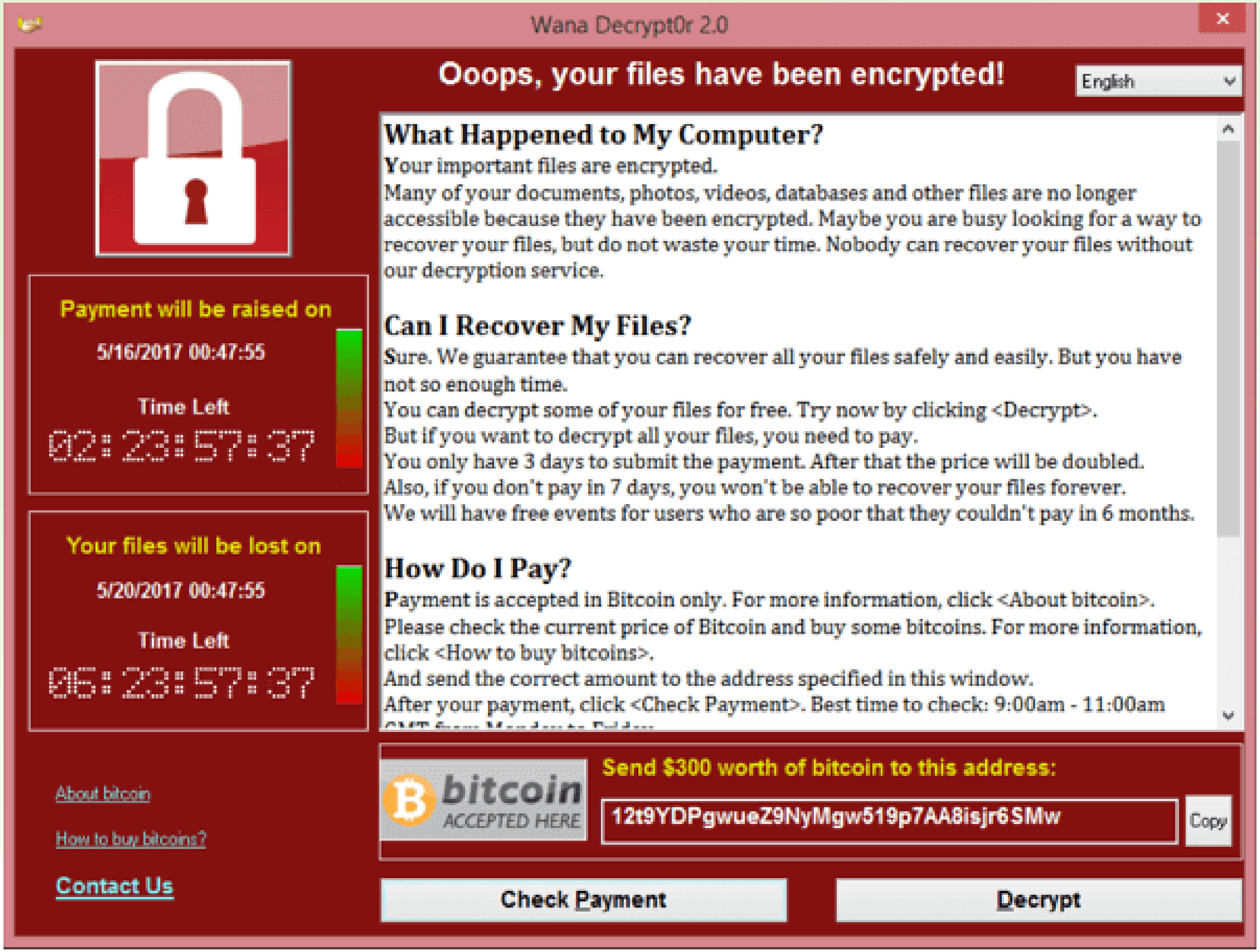


Dear Customer: KCB M-PESA soft loan is now Available at 0.5% interest, as from Ksh50,000/ 250,000/ Call, 0780000729. KCB MAKING THE DIFFERENCE.....

Thu 14:46 via SMS

INTERNET FRAUD

- **Ransomware:** A form of malware that restricts access to the compromised systems until a ransom demand is satisfied.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

CYBERSECURITY CHALLENGES

Lack of awareness

- Employees with limited knowledge of cybersecurity and are likely to be the victims of Cyber threats
- Increased generation of confidential customer data that is inadequately protected

Inadequate technical skills

- Insufficient technical skills, to identify cybercrime threats
- Inadequate protection mechanism in firewall, antimalware.
- Lack of adequate policies to address cybersecurity

CYBERSECURITY CHALLENGES

Low Prioritization.

- Low Prioritization from leadership
- Limited resources allocated to address the cyber security issues endangers vulnerable networks and their applications

Poor Technical Design

- Adversaries take advantage of poorly designed security infrastructure and simply bypass the poorly implemented application.

IMPACT OF CYBER CRIME

Loss of Revenue

- This loss can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organization. It can also occur when a business e-commerce site becomes compromised-inoperable, valuable income is lost when consumers are unable to use the site.

Data breaches

- Confidential data can be lost through cybercrime such as customer balances, customer names, transactions of customers, employee details and so on.

IMPACT OF CYBER CRIME

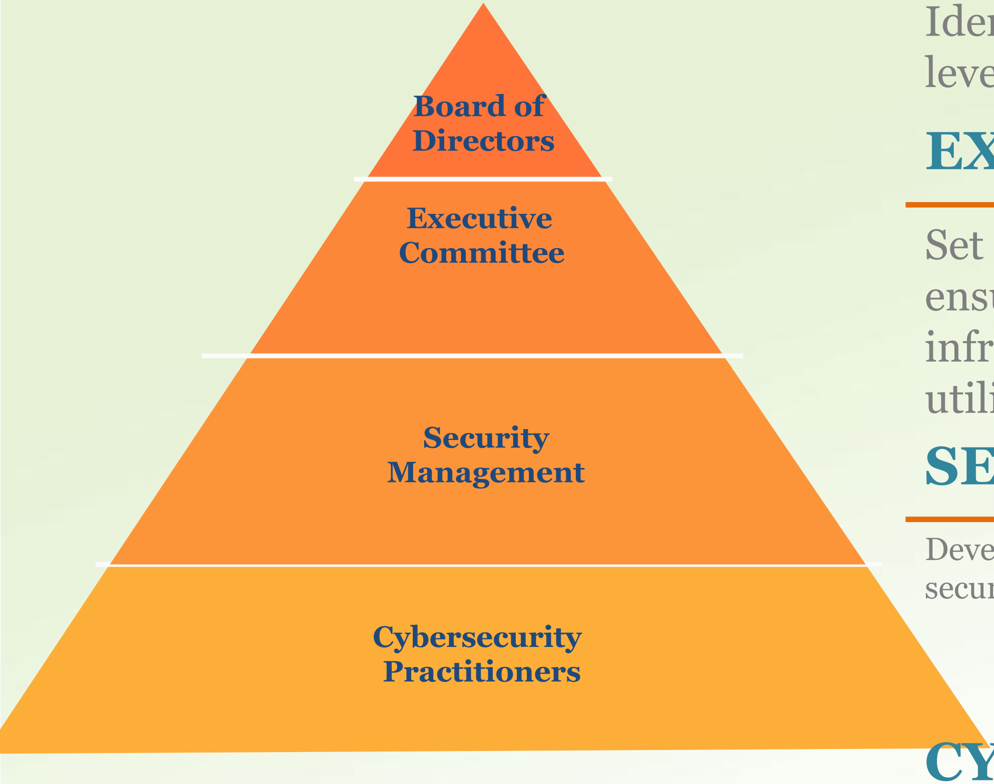
Reputational Damage

- Financial institutions heavily rely on trust and if there is any publicized cybercrime, then it is likely to reduce the ability of the organization to attract new customers or even retain old ones as they lose public confidence.

Regulatory fines

- Regulators are more stringent on organizations who don’t protect themselves from cybercrime and incases of breaches, they are likely to penalize such institutions

CYBERSECURITY ROLES



BOARD OF DIRECTORS

Identify key assets and verify that protection levels and priorities are appropriate

EXECUTIVE COMMITTEE

Set the tone for cybersecurity management and ensure that necessary functions, resources and infrastructure are available and properly utilized

SECURITY MANAGEMENT

Develop security and risk mitigation strategies, implement security programs and manage incidents and remediation

CYBERSECURITY PRACTITIONERS

Design, implement and manage processes and technical controls and respond to events and incidents

STRACT CONSULTING
Equipped to deliver

CASE STUDY

Anthem Insurance Company

CASE STUDY

About Anthem

Anthem, Inc., is the US health insurance giant behind brands like Blue Cross and Blue Shield, Anthem Insurance Company, Amerigroup, Caremore, and many others. The massive company employs more than 37,000 people and had a reported net income of $2.66 billion in 2012. Currently, Anthem is the second largest insurer in the United States.

What happened

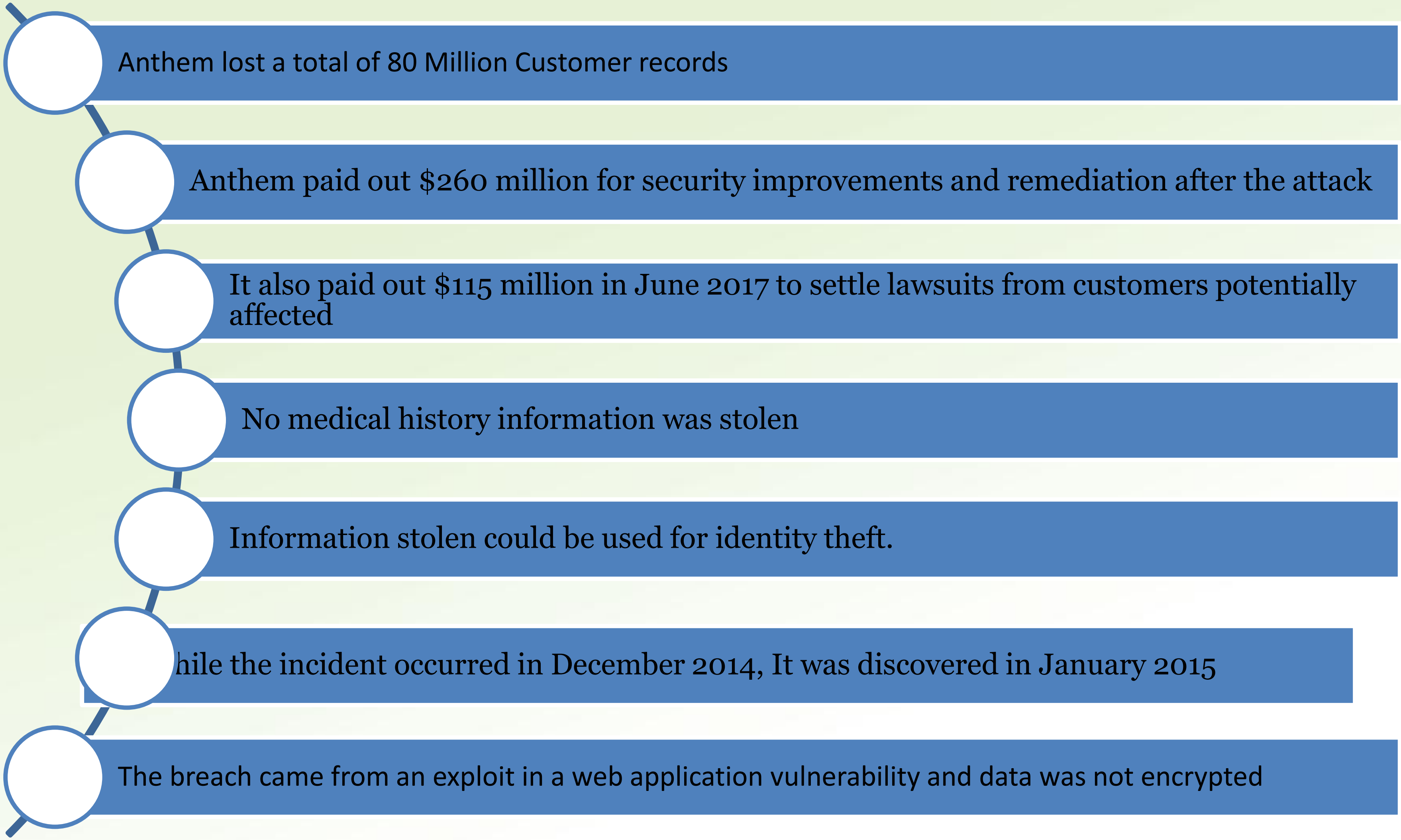
In December 2014, Anthem employees noticed suspicious database queries being made. Investigators confirmed unauthorized data queries to the company's servers on January 29, 2015.

In all, close to 80 million Americans have had their personal information exposed to hackers, with quite a bit of sensitive information being stolen. Hackers stole:

- Full names
- Physical addresses
- Email addresses
- Social Security numbers
- Birthdates
- Insurance membership numbers
- Medical IDs
- Employment information
- Income data

CASE STUDY

Anthem Cyberattack Facts and Figures



Anthem lost a total of 80 Million Customer records

Anthem paid out $260 million for security improvements and remediation after the attack

It also paid out $115 million in June 2017 to settle lawsuits from customers potentially affected

No medical history information was stolen

Information stolen could be used for identity theft.

hile the incident occurred in December 2014, It was discovered in January 2015

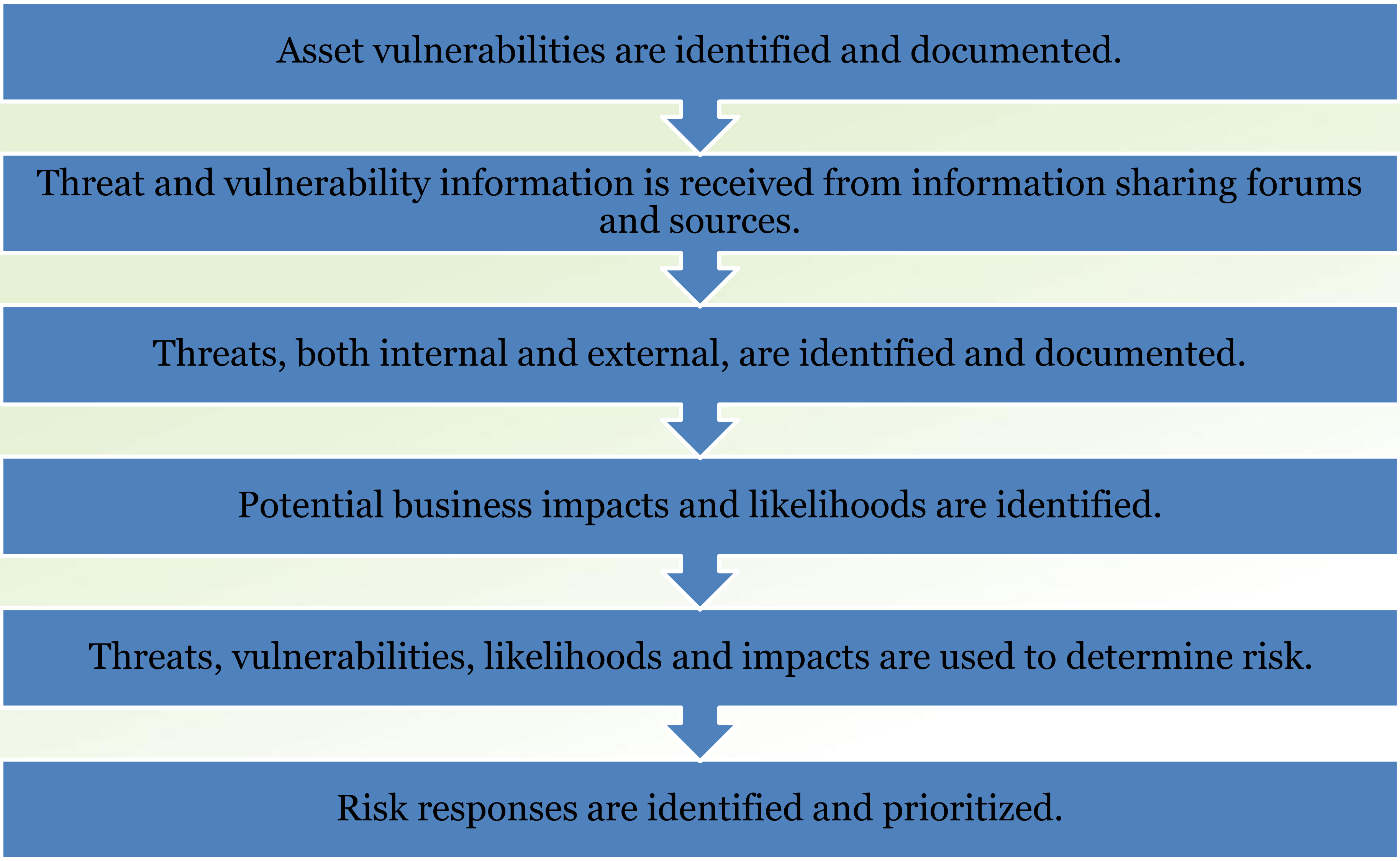
The breach came from an exploit in a web application vulnerability and data was not encrypted

Prevention of cyber attacks

- Organizational risk assessment
- Cybersecurity framework, strategy and policies
- Investment in human resources and tools to combat cyber threats
- Cybersecurity incident management
- Organization wide information security awareness and training
- Regular and independent compliance audits

STRACT CONSULTING
Equipped to deliver

Organizational risk assessment



Asset vulnerabilities are identified and documented.

Threat and vulnerability information is received from information sharing forums and sources.

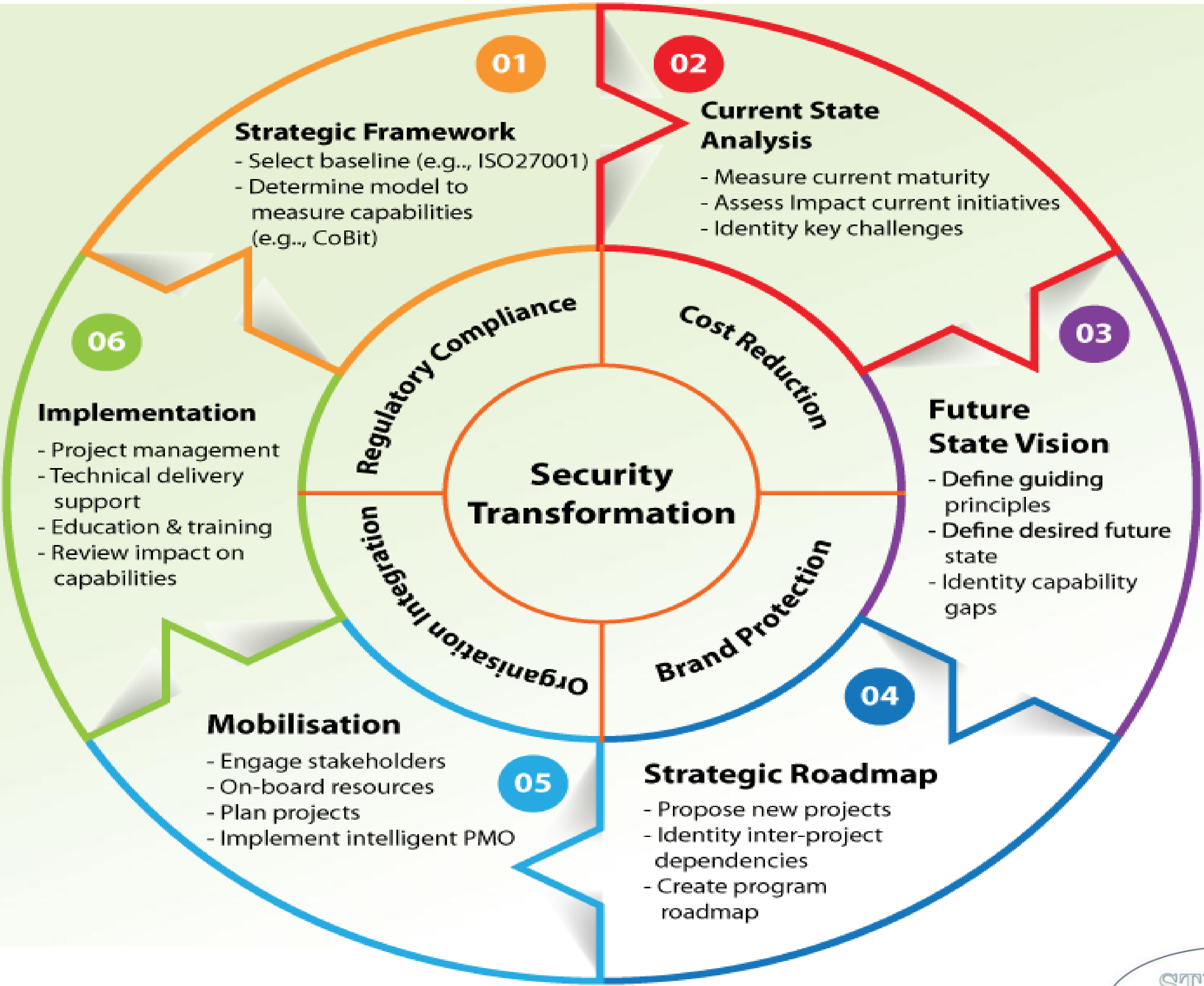
Threats, both internal and external, are identified and documented.

Potential business impacts and likelihoods are identified.

Threats, vulnerabilities, likelihoods and impacts are used to determine risk.

Risk responses are identified and prioritized.

CYBERSECURITY FRAMEWORK, STRATEGY AND POLICIES



01

Strategic Framework

- Select baseline (e.g.., ISO27001)
- Determine model to measure capabilities (e.g.., CoBit)

02

Current State Analysis

- Measure current maturity
- Assess Impact current initiatives
- Identity key challenges

03

Future State Vision

- Define guiding principles
- Define desired future state
- Identity capability gaps

04

Strategic Roadmap

- Propose new projects
- Identity inter-project dependencies
- Create program roadmap

05

Mobilisation

- Engage stakeholders
- On-board resources
- Plan projects
- Implement intelligent PMO

06

Implementation

- Project management
- Technical delivery support
- Education & training
- Review impact on capabilities

Regulatory Compliance

Cost Reduction

Brand Protection

Organisation Integration

Security Transformation

CYBERSECURITY INVESTMENT

1. INTRUSION DETECTION AND PREVENTION SYSTEMS

IDS and IPS tools help protect the wired and wireless networks against several security threat types. These technologies, like several other categories of network security tools, are being deployed with greater frequency as networks grow in size and complexity.

Both IDS and IPS solutions detect threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations. IDS tools passively monitor and detect suspicious activity; IPS tools perform active, in-line monitoring and can prevent attacks by known and unknown sources.

2. ANTI-MALWARE

Anti-malware network tools help administrators identify, block and remove malware. Malware is always on the lookout for network vulnerabilities .Best practices call for a multipronged defense that might also include IP blacklisting, data loss prevention (DLP) tools, anti-virus and anti-spyware software, web browsing policies, egress filtering, and outbound-traffic proxies.

3. MOBILE DEVICE MANAGEMENT

MDM software enhances network security through remote monitoring and control of security configurations, policy enforcement and patch pushes to mobile devices. Further, these systems can remotely lock lost, stolen or compromised mobile devices and, if needed, wipe all stored data.

CYBERSECURITY INVESTMENT

4. NETWORK ACCESS CONTROL

NAC products enforce security policy by granting only security policy–compliant devices access to network assets. They handle access authentication and authorization functions and can even control the data that specific users access, based on their ability to recognize users, their devices and their network roles.

5. NEXT-GENERATION FIREWALLS

This technology expands on traditional stateful inspection to provide next-generation network security services, including application visibility and control and web security essentials. Next-generation firewalls also improve on standard firewall capabilities through application-awareness features.

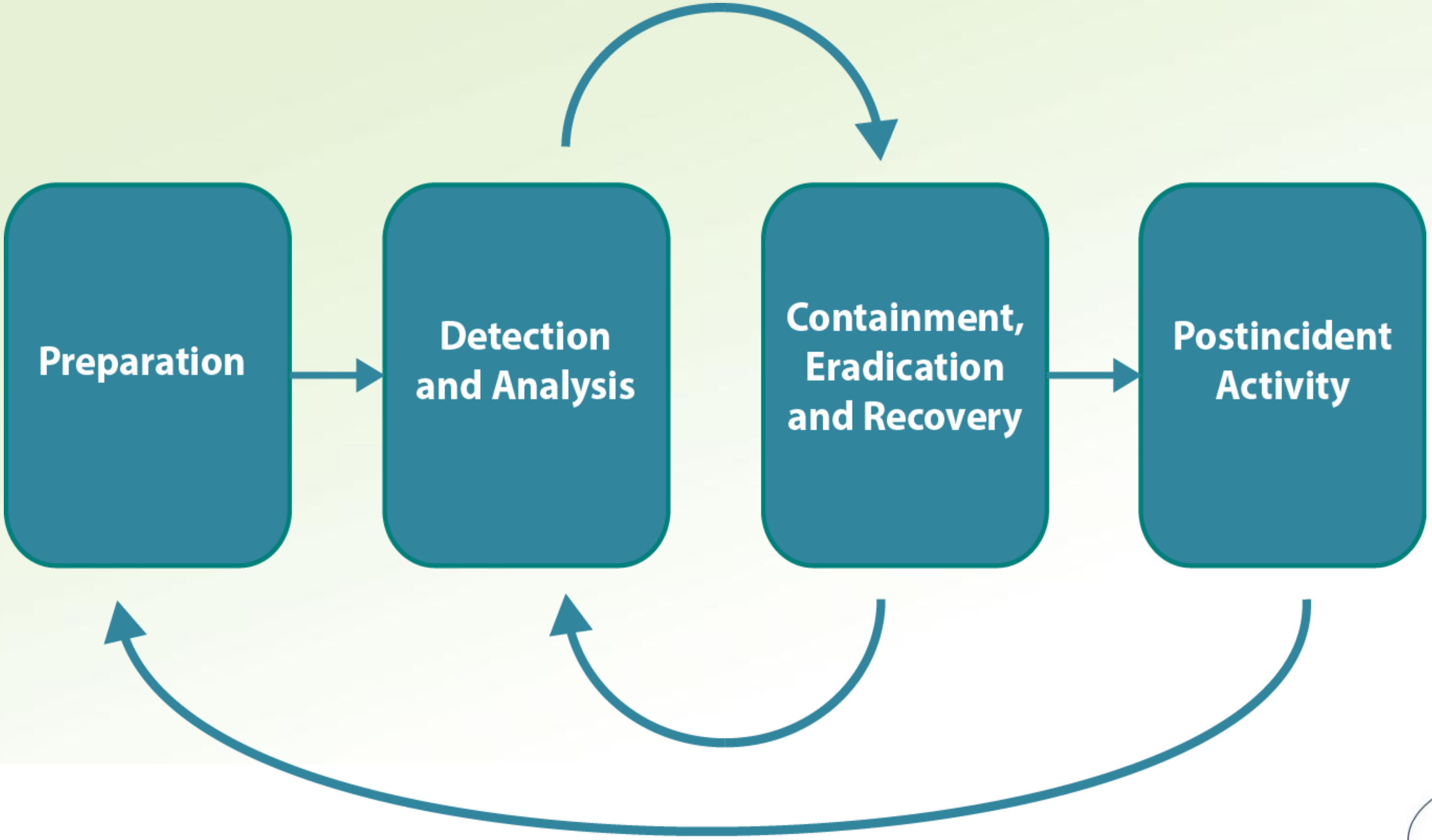
6. AUTHENTICATION AND AUTHORIZATION

Traditional directory-based services, such as Active Directory, authenticate users and grant access based on authorization rules. Newer identity-based security technologies manage authentication and authorization through such methods as digital certificates and public key infrastructure solutions.

INCIDENT RESPONSE PHASES

Incident response is a formal program that prepares an entity for an incident. Incident response phases are shown in below. Incident response generally includes:

1. **Preparation** to establish roles, responsibilities and plans for how an incident will be handled
2. **Detection and Analysis** capabilities to identify incidents as early as possible and effectively assess the nature of the incident
3. **Containment** capability if identifying an adversary is required
4. **Eradication and Recovery** procedures to contain the incident, reduce losses and return operations to normal
5. **Postincident Analysis** to determine corrective actions to prevent similar incidents in the future


Preparation

Detection and Analysis

Containment, Eradication and Recovery

Postincident Activity

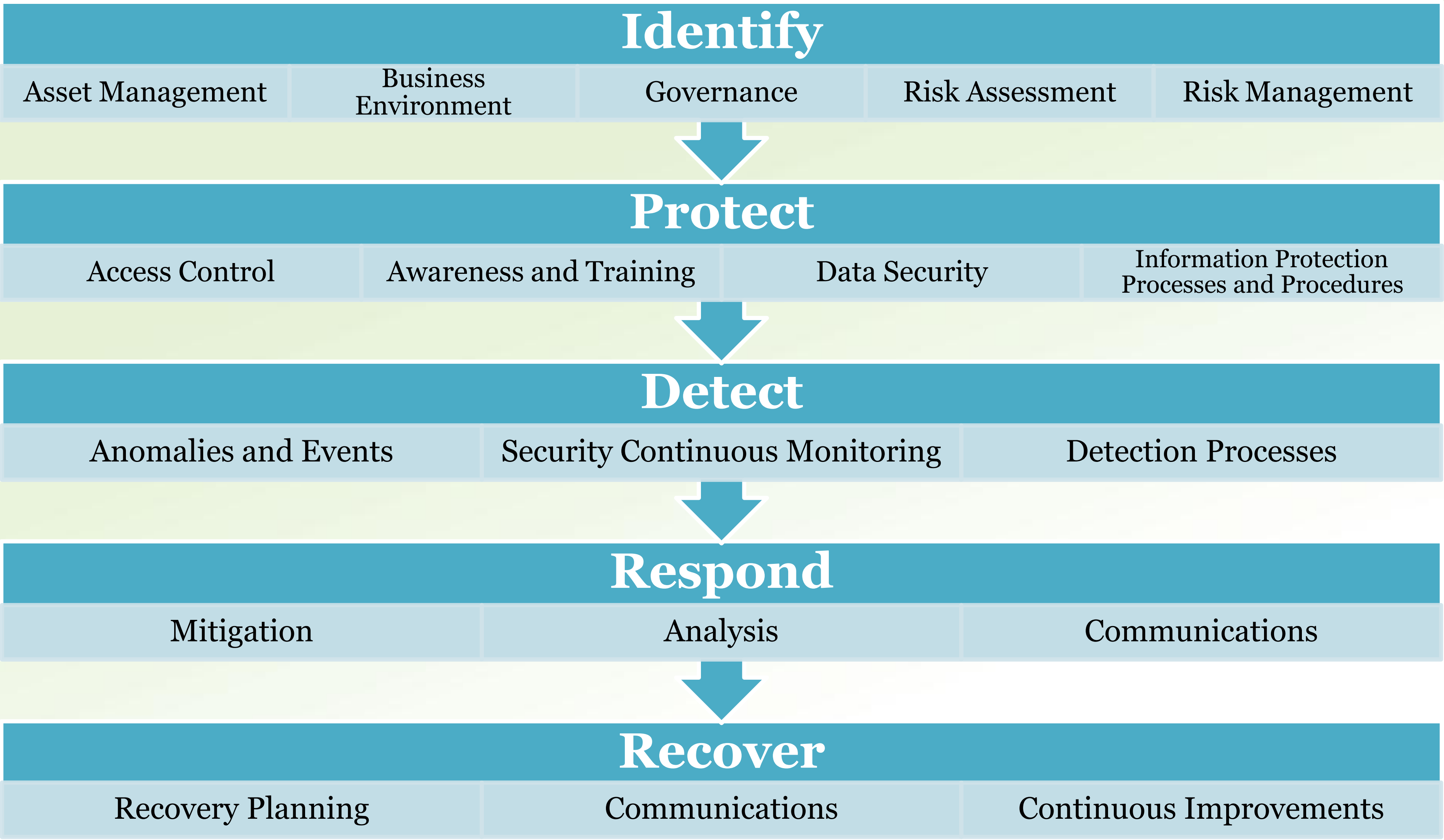
TRAINING AND AWARENESS

The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

- All users are informed and trained.
- Privileged users understand roles and responsibilities.
- Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities.
- Senior executives understand roles and responsibilities.
- Physical and information security personnel understand roles and responsibilities.

CYBERSECURITY AUDIT

The audit of your systems will include review



Identify

Asset Management | Business Environment | Governance | Risk Assessment | Risk Management

Protect

Access Control | Awareness and Training | Data Security | Information Protection Processes and Procedures

Detect

Anomalies and Events | Security Continuous Monitoring | Detection Processes

Respond

Mitigation | Analysis | Communications

Recover

Recovery Planning | Communications | Continuous Improvements

CYBERSECURITY OPPORTUNITY

Providing Cybersecurity insurance is a growing business

First party insurance

- First-party insurance typically covers
  - Damage to digital assets
  - Business interruptions due to outages on the computer systems
  - Cyber extortion through Ransomware
  - Reputational harm

Third party insurance

- Third-party insurance covers
  - Liability and cost of forensic investigations
  - Customer notifications
  - Credit Monitoring
  - Public Relations
  - Legal defense
  - Compensation
  - Regulatory fines

Key Considerations

- As it is a new area, various elements are still unclear
  - Intellectual property theft coverage
  - Reputational harm considerations
  - Actuarial data based on security controls implemented

Thank You