Cyber- Attacks:
The New Frontier for Fraudsters

Daniel Wanjohi,
Technology Security Specialist

What is it All about

The Cyber Security Agenda ;

- Protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

- Any Organization has the mandate to ensure the Availability, Confidentiality and the Integrity of all the systems that support their business processes.

Cyber crime

What is it?

Using the Internet/Computer device to commit a crime.

Identity Theft, Hacking, Online Stalking, Stealing information……and the list goes on.

The Current Landscape

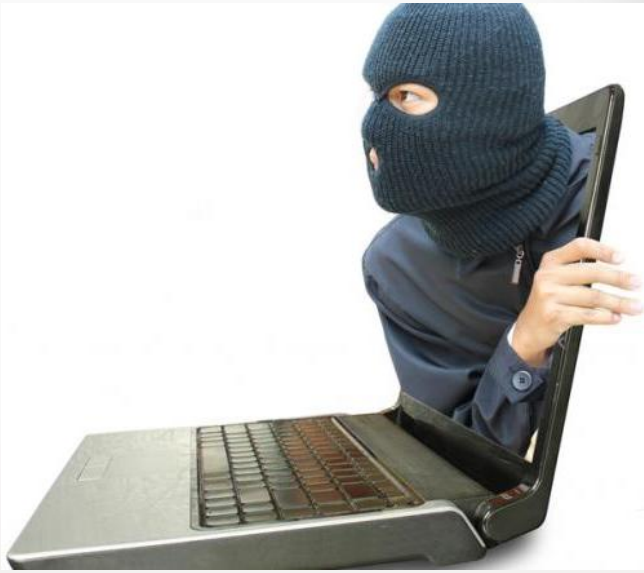
Focus on Kenya in the last one year

- SIM Swap Fraud (Telcos)
- The NIC Incident
- The NYS Saga
- ….and many more that are not bold enough to open up ☺

The Motivations

What are hackers after

- Adventure/Ego/Challenge
- Business Disruptions
- Hacktivism (political reasons)
- Economic Reasons



Possible Avenues

How most cyber crime is propagated

- Malware
- Denial-of-service (DoS)
- Phishing and Spam
- Social Engineering
- Identity Theft
- Drive-By-Downloads
- Potentially Unwanted Programs
- ……etc

What the future Holds

Cybercrime can only get worse ☹

- Internet growth
- Mobile adoption
- A surge in E-commerce
- Internet of Everything
- Corporate Espionage & Cyber Terrorism

The Net Effect

Possible outcomes of cyber crime

- ✓ Reputation loss
- ✓ Intellectual property loss
- ✓ Legislative Breaches leading to legal actions
- ✓ Loss of customer confidence
- ✓ Business interruption costs
- ✓ Financial loss

Financial Implications

Costs to the Organizations

- Costs in anticipation of cyber crime.
- Costs as a consequence of cyber crime:.
- Costs in response to cyber crime
- Indirect costs associated with cyber crime

  e.g. reputational loss

The Hurdles

Challenges in Curbing Cyber Crime

- Wrong prioritization as a low risk in Business.
- Difficult to trace and un-earth (Anonymity of the internet).
- Shortage of Cyber-Security skillset
- Inadequate laws governing Cyber crime
- Jurisdictional issues

Way Forward

Tangible steps in Curbing Cyber Crime

Begin with a Risk Assessment in order to.

- ✓ Establish a Roadmap for the cyber security journey.
- ✓ Create a Baseline for compliance.
- ✓ Provide Due Diligence to all actors
- ✓ Finds the Weak Areas that need to be addressed

How to Identify the risks

- **Holistic Approach**
  - ❖ Comprehensive reviews (infrastructure, server, application, etc.)
  - ❖ Consider people and processes, as well as technology
- **Documentation**
  - ❖ Create awareness to staff: with clear standards, policies and specific recommendations.
- **Threat Modeling**
  - ❖ Identifying assets and Corresponding threats
  - ❖ Perform qualitative (or quantitative) assessments of risk

Common Risk/Exposure Areas

- ✓ Policies & Procedures
- ✓ Access Control
- ✓ Patch Management
- ✓ Auditing and Logging
- ✓ Mis-Configured Systems & Applications
- ✓ Incident Handling Processes
- ✓ Disaster Recovery & Business Continuity

Security Policies & Awareness

- ✓ Policies communicate the Organizations Commitment to Security
- ✓ Provide a Baseline and Roadmap for Security Controls
- ✓ Define the Auditing and Logging Standards

!

Policies are only as effective as they are communicated and enforced in an organization

Available Frameworks that can set us off in the creation of policies include.. ISO 27001 & SSAE 16

Access Control

- ✓ Defines who, how and what happens when users access systems.
- ✓ Helps deal with risks such as weak passwords, accounts sharing, inactive/idle accounts etc.
- ✓ Drives the use of more stricter controls and secure technologies
  - Authorization, Authentication and Accounting Mechanisms (AAA), Two-Factor Authentication, complex passwords etc.

Patch Management

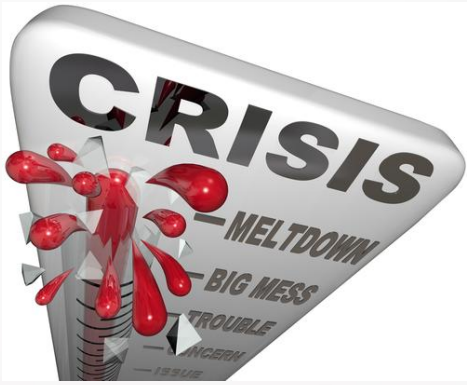
- ✓ There is a tendency that most software stays un updated.
- ✓ New software exploits and vulnerabilities are being released daily .
- ✓ A Properly defined patch management program needs to include:
  - Strong and enforceable Patch Management procedures
  - Automated Intrusion Prevention Mechanisms

Mis-Configured Systems

- ✓ Most Systems will be deployed with inherent loopholes/ default settings
- ✓ Possible best practices …..
  - Avail only the needed or updated Services
  - Protect/Hide your Wireless Networks
  - Remove Default Settings and software configurations
  - Tight Access controls at Firewall (allow only what is required)
  - …..and many more

Incident Handling Processes

- ✓ Even as the organizations strives to prevent cyber threats, they must be incident ready.
- ✓ Well defined incident procedures must outline.
  - – Intrusion Prevention/Detection
  - – Anti-malware Mechanisms
  - – Logging/Auditing (incident analysis)
  - – Strong Policies and Documentation



Disaster Recovery & Business Continuity

- ✓ Defines how to sustain operations in case of system failure.
- ✓ A matured Disaster Recovery & Business Continuity plan must have;
  - Formal Plan
  - Prioritized Systems
  - Standard Backup procedures
  - Tested Recovery mechanisms
  - Redundant Systems

dwanjohi@safaricom.co.ke