Covenant University Town & Gown Seminar 2015

Information Security in Business: Issues and Solutions

A Covenant University Presentation

By

Favour Femi-Oyewole,

BSc, MSc (Computer Science), MSc (Information Security)

Certified COBIT 5 Assessor /Certified ISO 27001

(1st Female COBIT 5 Assessor Certified in Africa)

March 2015

1. Introduction
2. Definitions
3. The Role of a CISO
4. The need for CISO
5. CISO and the Business - Issues
6. CISO and the Business - Solutions
7. Defense in Depth
8. Scenarios
9. Q & A
10. Closing Thoughts

INTRODUCTION

Information security is the process of protecting the availability, confidentiality, and integrity of data.

No security system is foolproof, but taking basic and practical steps to protect data is critical for good information security.

Information Security is not complete without addressing the key components of strategy, people, process, technology and compliance.

DEFINITION

Information

- A collection of organized fact
- A key resource for all enterprises.

Security

- Lock the doors and windows and you are secure (No)
- Call the police when you feel insecure (Really?)
- Computers are powerful, programmable machines (Whoever programs them controls them (and not you)

Information Security

- Information Security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Assets

- Something you own that has value
- Can gain value over time
- Can lose value over time

DEFINITION

Threat

- The potential to cause unauthorized disclosure, changes, or destruction to an asset.
  - Impact: potential breach in confidentiality, unavailability of information, and integrity failure
  - Types: natural, environmental, and man-made

Vulnerability

- A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats.

Risk

- Risk is generally defined as the combination of the probability of an event and its consequence
- Information risk is a business issue and the CISO's role is to enable those discussions and support sensible business decisions.

Cyber Security

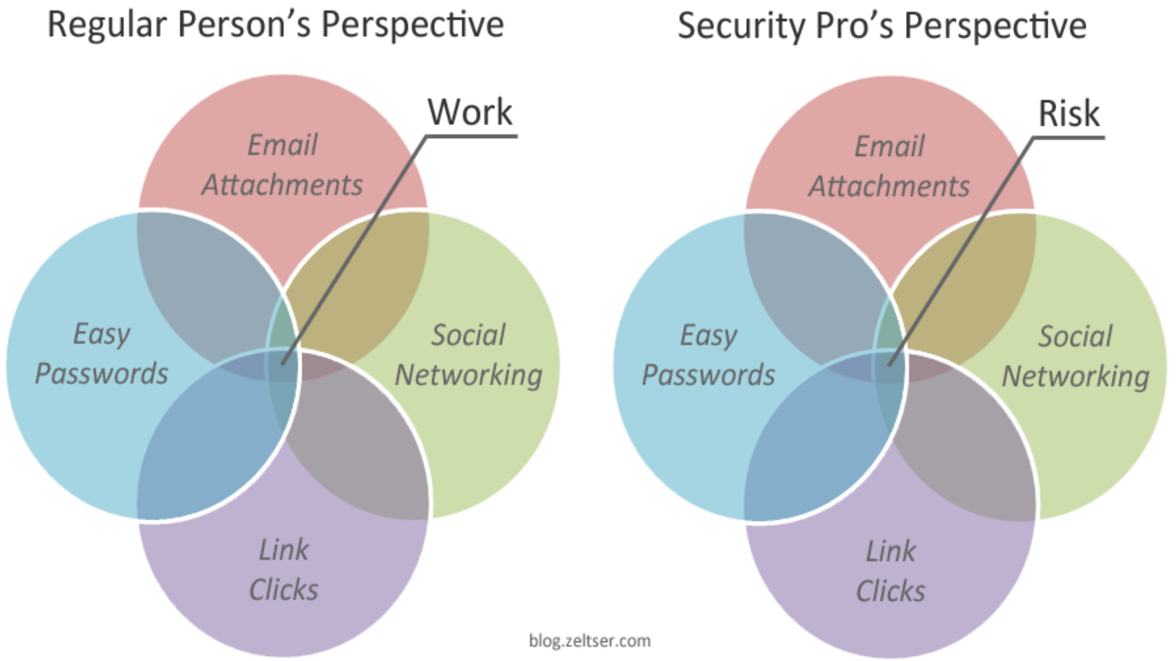
- Cyber security is the body of technologies, processes and practices [information technology security] designed to protect networks, computers, programs and data from unintended or unauthorized access, change or destruction.

The Role of a CISO

CISOs (***Chief Information Security Officers***) are responsible for establishing a strategy, execution of that strategy, risk management, communicating effectively with senior executives and business leaders, complying with regulators, and leading the charge against escalating cyber threats using various security technologies.

The need for a CISO

No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a Security Program by Information Security professionals



blog.zeltser.com

CISO and the Business – Issues

- Speak the Boardroom Language - Executive leaders are asking CISOs to be strategic thinkers as well as IT administrators.
- In other to become successful in the role of CISO - CISOs will need to understand and influence business risk decisions and be involved with everything from developing privacy policies to preparing disaster recovery plans
- Emergence trends - the threat landscape continues to grow while budgets and access to skilled resources get harder to come by.
- Budget-strategy disconnect - . They may not control the budget and may not be the ultimate decision maker.

- CISOs are concerned about the intensity, volume and complexity of cyber threats that run the gamut from malicious code to zero-day attacks.
- CISOs face various internal challenges when procuring security solutions. They need to justify the purchase and deal effectively with internal stakeholders.
- CISOs always have the technical awareness but may not have procurement authority. But CISOs are always influencers; they impact everyone in a company because the security organisation is pervasive in all departments and business functions.

Risk Issues?

Understanding Risk Appetite

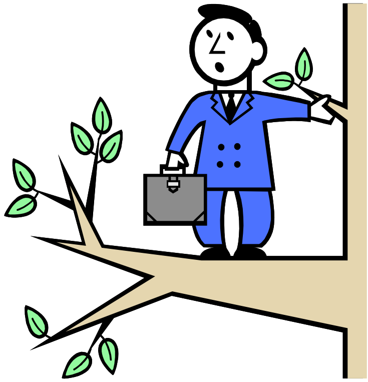
Understanding Risk Acceptance (Who)

Understanding Threats and Vulnerabilities

Control Linking

Understanding Residual Risk

Understanding the Risk Process



Ensuring the correct people are involved

Understanding Control Infrastructures

Risk Assessment –v- Risk Management

Accepting Residual Risk

Risk Reporting

Understanding Control Selection process

Cost of Remediation

Risk Differences:
Fraud
Business
Financial
Technology
Process
People
Tax
Governance

Risk Mitigation

Risk Integration – Linking it all together

Risk Issues? Internal Threats

Port Security
"USB"

Information
leakage

Spam

Sniffing

Webmail

Gopher

Social Engineering

Rogue Applications

Access Control

Sabotage

Instant
Messaging

HTTP

Too many Services

Admin Errors

Sendmail

IP Theft

Privilege Escalation

Security Sensor Misconfiguration

Education and Awareness

Disgruntled Employees

Modem Hijacking

Bad Application Code

Patch Management

Policy adherence

UDP Services

News

Unauthorized Insider access

TFTP

FTP

Identity theft

External DNS Zone Transfers

Finger Buffers

Human Factor

TCP Hijacking

Wireless

NFS

email

DNS Cache-based Trust

Poorly Maintained System

Risk Issues? External Threats

Remote Control Tools

Hackers

Process Hijacking

Website Attacks

Social Engineering

Backdoor ownership of Host machines

Terrorism

Dumpster Diving

Hostile Code

Sniffing

Buffer Overflows

Theft of Trade Secrets

Breach of Physical Security

Crackers

DoS/DDoS

Spoofing

Identity theft

Industrial Espionage

Rogue Applications

Trojan Horses

Worms

New Regulations

Script Kiddies

Labor Action

WarGames

Virus's

Intrusion to commit a Felony

Human Factor

Foreign Government Espionage

Abuse of Civil Authority

Denial of Service Attacks

Data Lineage

Legacy Systems

Hostile Java Applets

Hostile VB Scripts

ECHELON/CARNIVORE – Government Surveillance

IP Theft

Compromise of centralized 3rd Party Data Repositories

Risk Issues? Physical

Cable Security
Building Management
Disposal Services
Anti-theft measures
Guarding
Perimeter Security
Business Continuity
Physical Protection
Trash collection
Express Kidnapping
Surveillance
Wireless
Chauffeurs/Drivers
Maintenance
Snooping
Elevators
Special Projects
Protection (People)
Access Control
Parking Lots
Utilities – Power and Water
Communications
CCTV
Booms
Telephony
Patrols
Smoking/Smoke Areas
Alarms
Contracts
Reception
Keying
Bugs & Probes
Keycards
Building Security
Evacuation
Emergency Services
Transportation
Escorting
Health & Safety
Cleaning Staff
Counter Surveillance
Entry/Exit Points
Landlords
Fireams
Turnstiles
Plants
Raised Flooring
Proximity Security
Clear Desk
Disaster Recovery
Office Erection
Fireproof Safes
First Aid
Biometrics
Entry/Exit Controls
Emergency Exits
Physical Layouts
Eavesdropping
Fire-resistant and tamper-resistant storage facilities
Anti-vandal measures

Risk Issues? Security issues

Intrusion Protection

Data Classification

Security Management

Security Health Checks

Security Measurement

Portal Security

Mobile Computing

Security in Enterprise Architectures

Network Forensics

Website Protection

Security Infrastructure

Patch Management

Disaster Recovery

Legacy Systems

Data Exchange

HR Policy

Log Analysis

Collaboration/Partners

Event Correlation

Legal/Regulatory

Privilege Management

Malware

Domain Security

Computer Forensics

Risk Assessments

Training

Webmail

Intrusion Detection

Control Standards

Wifi

Platform Security

Security Awareness

The Human Factor

Content Management

Virus

Risk Analysis

Encryption

Firewalls

PKI Readiness Reviews

Secure Email

Security Frameworks

Asset Classification

Corporate Governance

Users

Consultants

Security Integration

Event Monitoring

Vulnerabilities

Incident Management

PKI Infrastructures

Privacy

Security Baselines

Security Policies and Procedures

Business Continuity Planning

Data Lineage

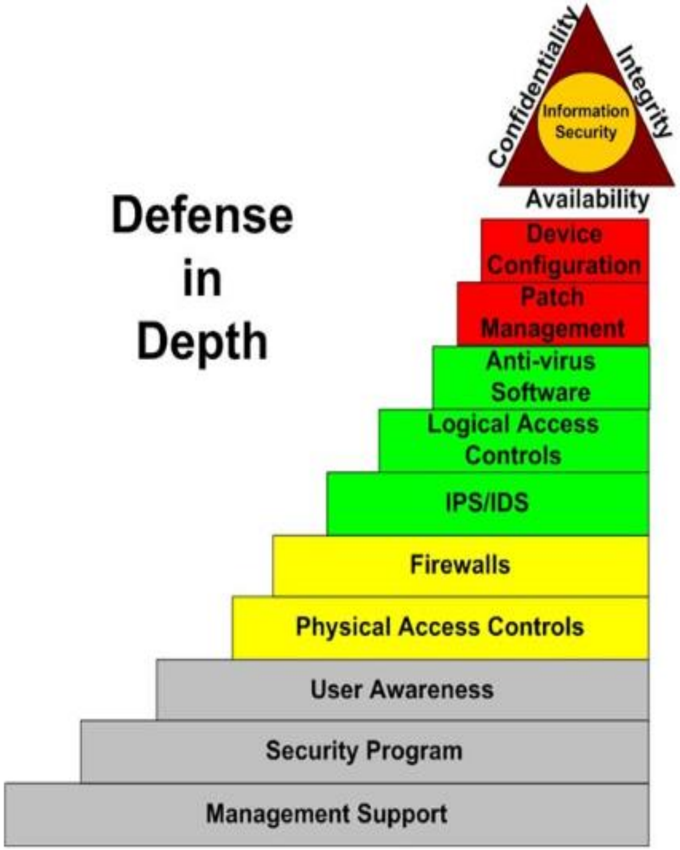
Mainframe Security

CISO and the Business – Solution

- Security must be considered a growth engine for the business. Security should never be a roadblock or hassle that undermines user productivity and stands in the way of business innovation
- Security must work with existing architecture, and be usable. Security teams should not have to create or re-build an architecture to accommodate new technology solutions that are meant to improve security.
- Security must be transparent and informative. Users should be presented with information that helps them understand why security is stopping them from taking a particular action.
- Security must enable visibility and appropriate action. Security solutions with open security architecture enable security teams to determine whether those solutions are truly effective.
- Most organizations have approached cyber security by trying to put increasingly sophisticated defences around their perimeter. The reality is that a motivated attacker will likely find a vulnerability—or an employee may inadvertently create an opening therefore Security must be viewed as a “people problem.” A technology-centric approach to security does not improve security; in fact, it exacerbates it.

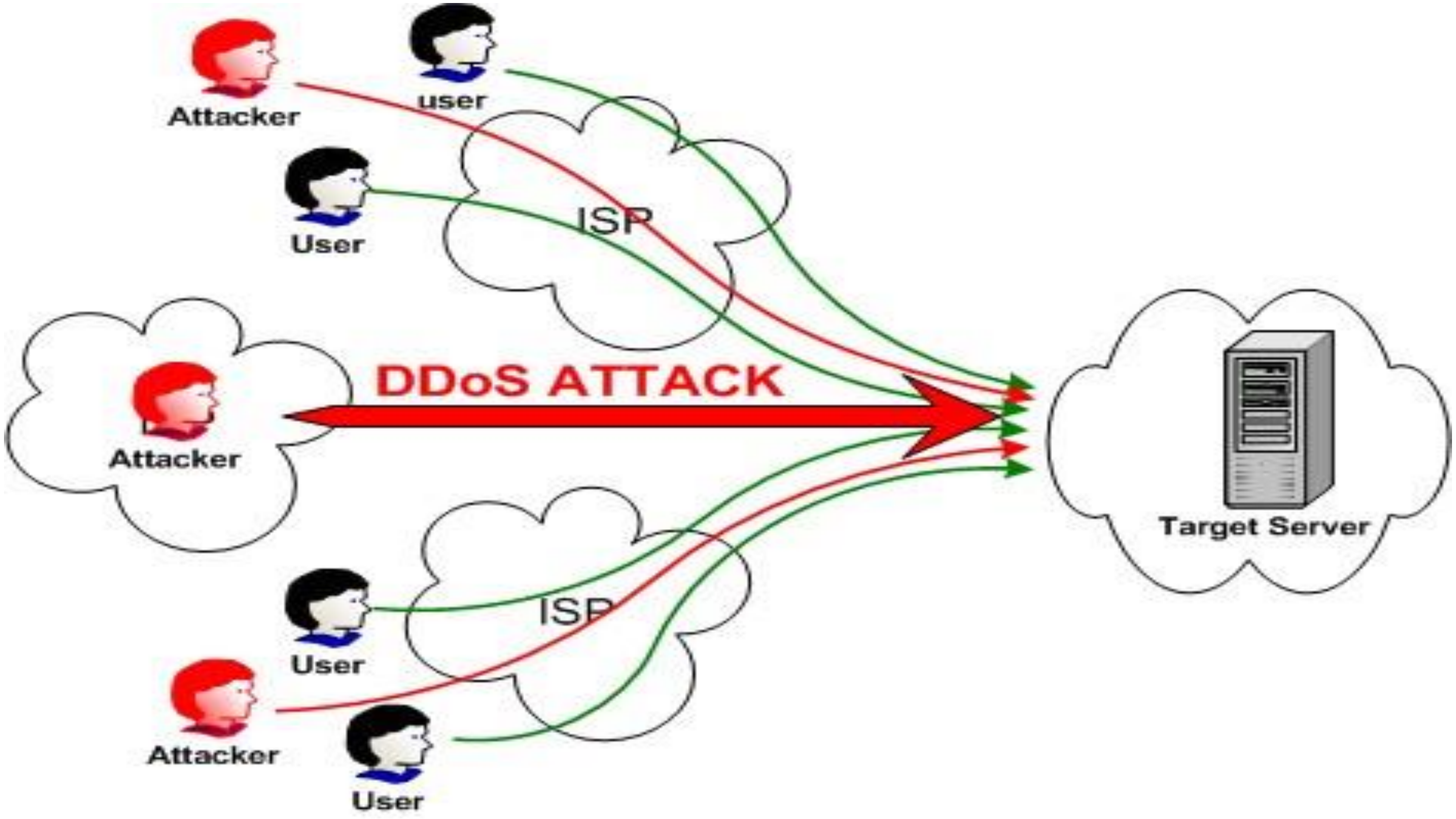
Defence in Depth

- Malware Detection & Mitigation
- Mobile Security
- DDoS Prevention & Remediation
- Network Visibility
- Cloud Services
- Identity & Access Management
- Compliance Program Development
- Threat Intelligence -
- Information Security Program Model



Defence in Depth

Distributed DoS (DDoS) Attack



Closing Thoughts

Information Security is a journey not a destination and there will always be new ways of doing things, new threats, new vulnerabilities, new methodologies, new technologies and countermeasures…

- ❑ Security is never a destination but a journey
- ❑ Never forget Security is YOU and YOU are security
- ❑ Do not be the weakest link that breaks the CHAIN

Security is everyone's RESPONSIBILITY.

Summary

- Cyber security has come to stay with us

- There is no 100% security, it is a continuous process and journey without a destination

- Everyone is involved, it’s a shared responsibility

Questions?