Managing cyber-risk with Regulations

By
Ayo Rotibi
(Information Security Consultant)

Relevant Statistics

- NIGERIA
  - 155,215,573 population (2011) - Country Area: 923,768 sq km
  - 45,039,711 Internet users (ITU, 12/2011)
  - 4,369,740 Facebook users (ITU, 12/2011)
- Gartner Research 2011
  - 5.5M web pages infected with *MALWARE* in 2010
  - 97% of Businesses uses Desktop Antivirus
  - 98% of Businesses have Firewalls
  - Yet, 65% suffered from various outbreak in 2010

Cybersecurity Defined

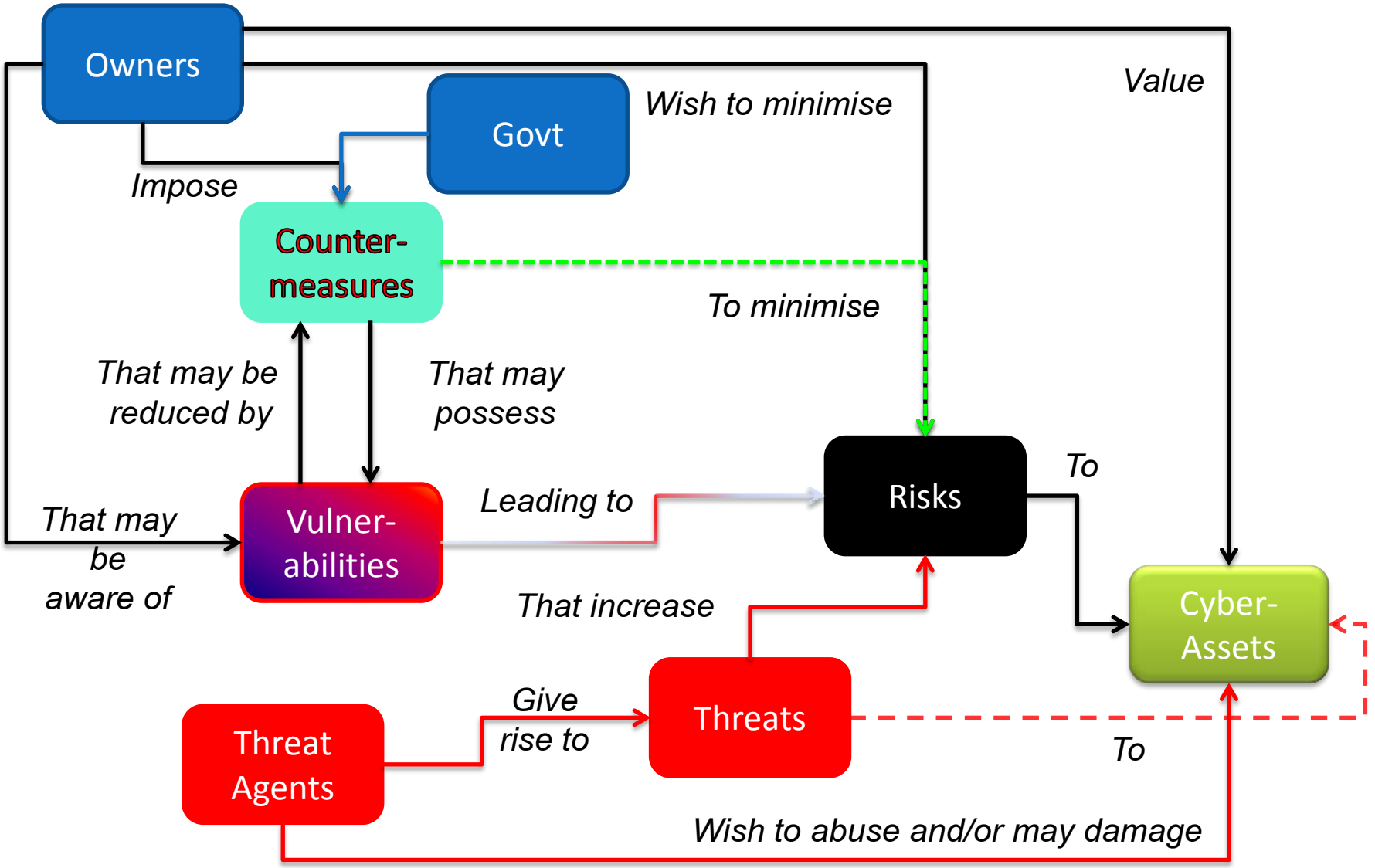
The term `cybersecurity' means the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

(Homeland Security Act, Section 17(A) as Amended 2004)

Cyber (Information) Security

- CIA Model - Three Concepts:
  - Confidentiality
  - Integrity
  - Availability
- Information Assurance – Five Objectives to achieve Five Concepts:
  - Information Operations that protect and defend information and information systems by ensuring their confidentiality, authentication, integrity, availability, and non-repudiation. This includes providing for restoration of information systems by incorporating *protection*, detection and reaction capabilities.

Cyberscurity in Context



Challenges

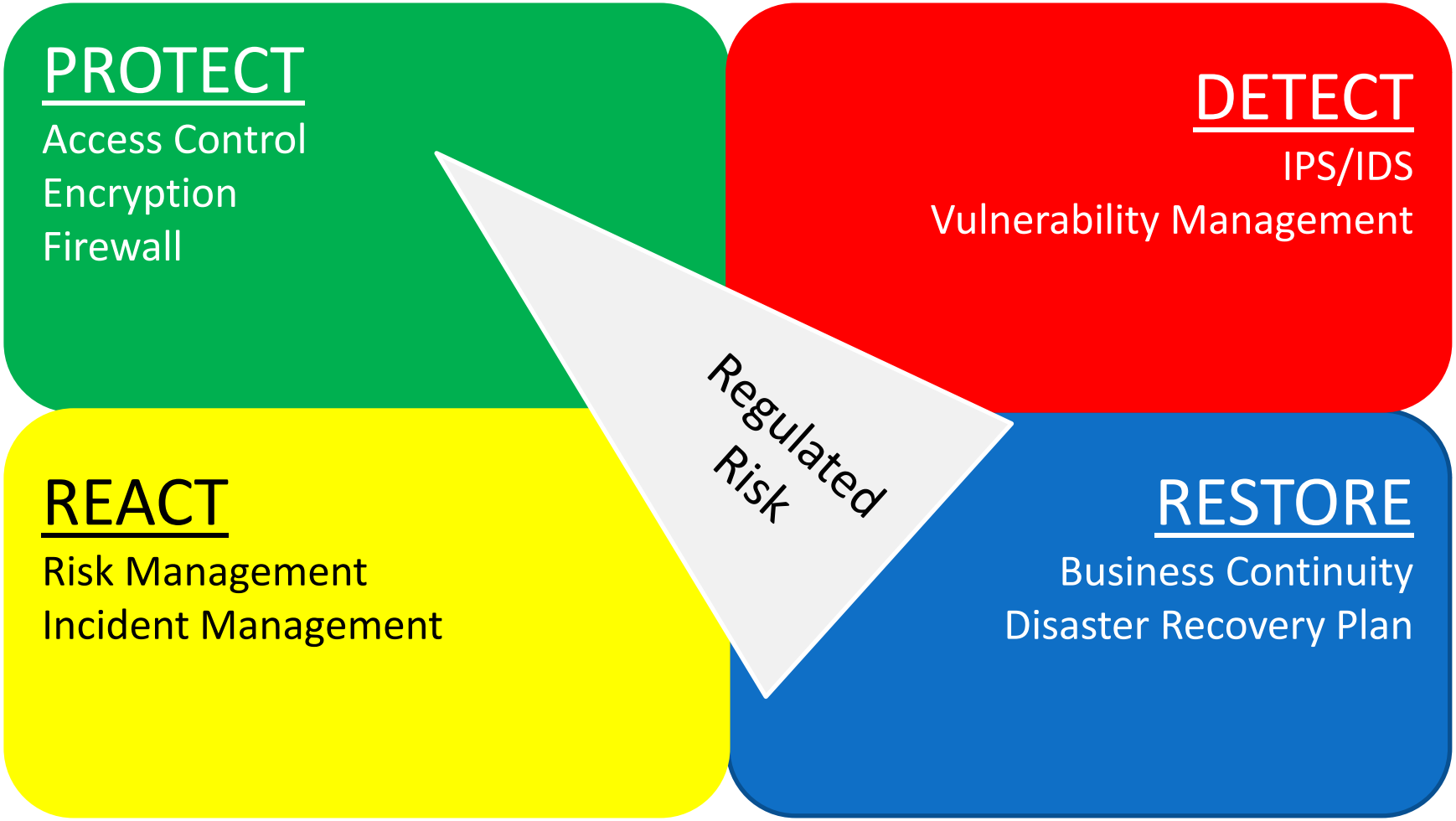
- Global:
  - Computer and network security is complex
  - The threats and vulnerabilities are complex
  - The countermeasures are complex
  - The products that organizations need to buy to mitigate the risks are complex
  - Security is primarily visible only when it fails
  - Lack of visibility across various risks and threats
  - Information Security viewed as technology issue
- Nigeria:
  - No existing standards on ICT operations
  - No visibility of cyber-incident

Cost of Security Breach

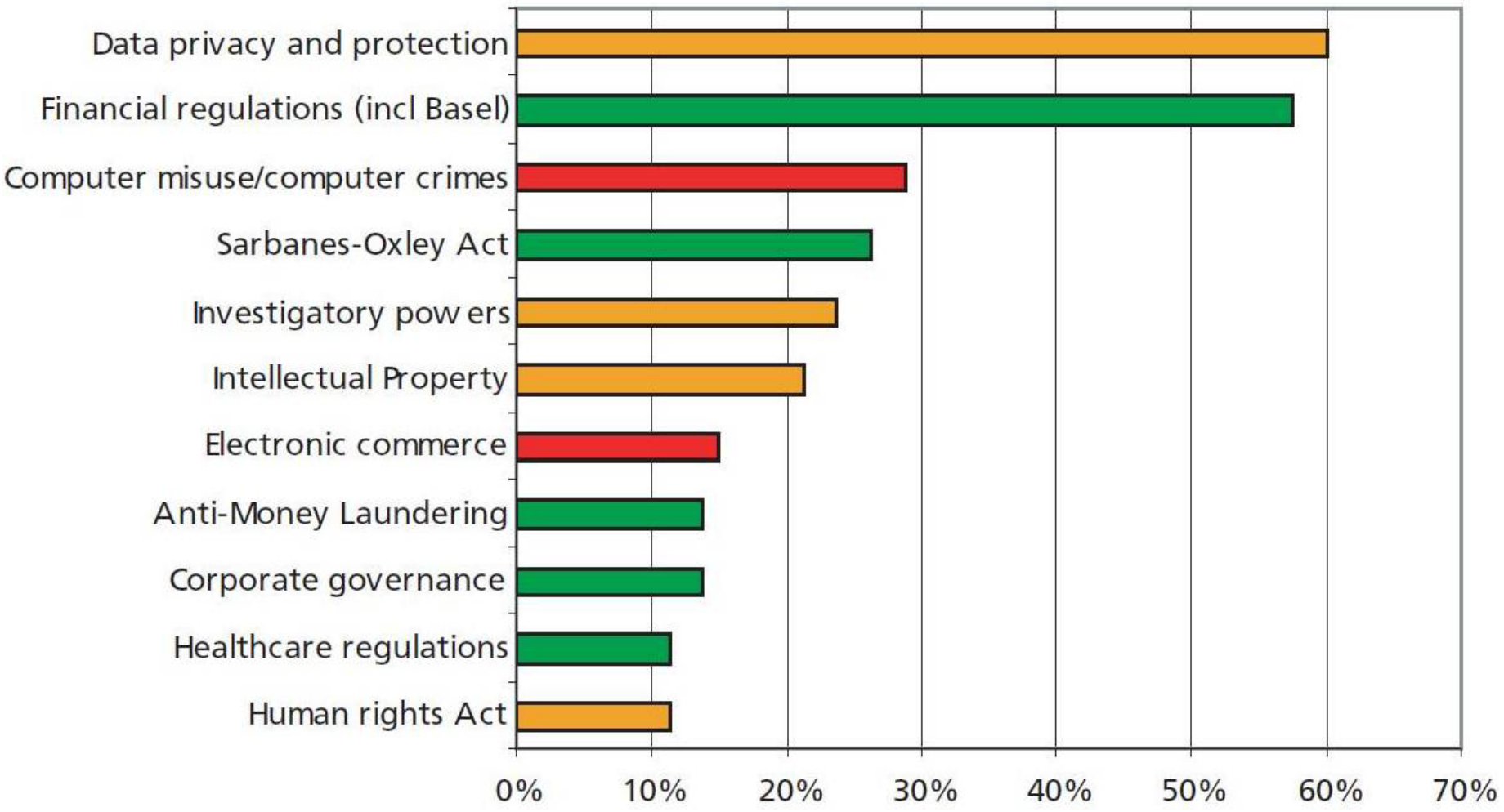
- Global Cybercrime Cost - $400B (2010)
- Average cost per record - $90 to $305 *(Forrester)*
- Breach Recovery time - 18 to 45 days + $416K
- One laptop stolen every 53 seconds *(Gartner)*
- Brand rebuilding:
  - PR Consulting fees, Advertising campaigns, Liability suits, Customer outreach efforts
- Case Study
  - I LOVE YOU virus – Loss of $6.7B in the first 5 days
  - TJMax - $1.7B + Legal cost
  - Dept. of Veteran Affairs - $26.5B
  - Sony - $171M to cleanup

Risk Management by Regulations

CYBER-RISK AND CYBER-REGULATION



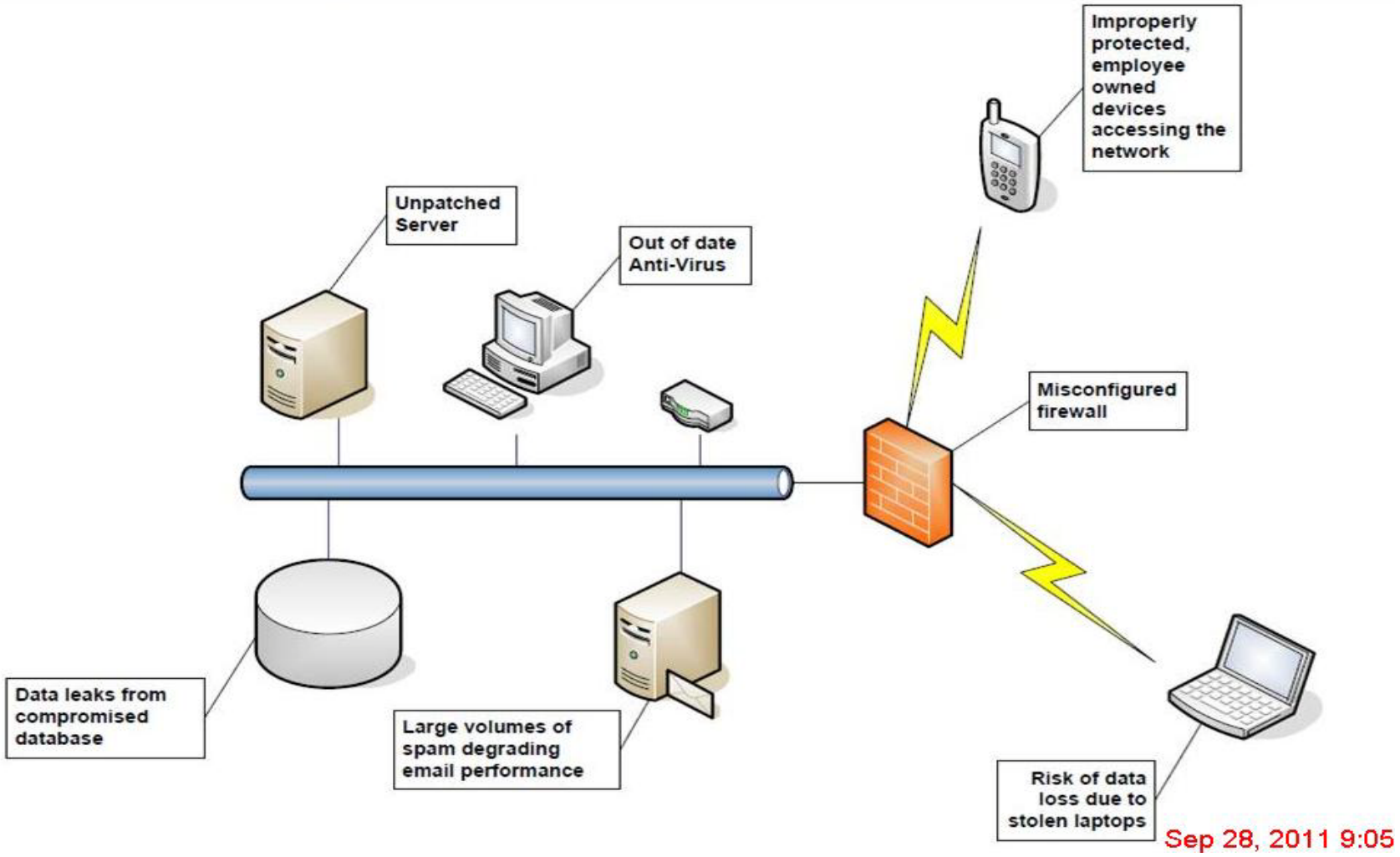
Laws/Regulations relevant to information security



Case Study – PCI DSS

- **Build and Maintain a Secure Network**
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- **Protect Cardholder Data**
- Requirement 3: Protect stored cardholder data.
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
- Requirement 5: Use and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
- Requirement 12: Maintain a policy that addresses information security for employees
- and contractors.

How are you fearing?



Conclusion

- Regulations demands compliance
- Compliance inspires governance
- Governance enables sound Business Alignment
- Alignments brings Profit
- Profit means Good Business
- Therefore REGULATIONS = GOOD BUSINESS

Cyber (Information) Security

- CIA Model - Three Concepts:
  - Confidentiality
  - Integrity
  - Availability
- Information Ass… …ives to achieve F…

Cyber Security = Good Business Sense

…ons that protect and defend …and information systems by ensuring their …dentiality, authentication, integrity, availability, and non-repudiation. This includes providing for restoration of information systems by incorporating *protection*, detection and reaction capabilities.

Contacts

- Email: ayo.rotibi@isecureconsulting.co.uk
- Mobile: 0810 963 1473, 0818 770 4842