Beyond Compliance: Managing Technology and Cybersecurity Risks

Rural Bankers Association of the Philippines
60th Charter Anniversary Symposium
23 – 24 October 2017

BANGKO SENTRAL NG PILIPINAS

Video Presentation

Cyber Threats on the U.S. Banking Industry

Source: https://www.youtube.com/watch?v=YQTzh9VR_xU

WHAT STRIKES A CHORD?

"The sophistication and seriousness of the attacks on the financial system and elsewhere are ever increasing."

"We could be heading towards a massive cyber-attack on our banks and insurers."

"Armageddon"

"Those hacks cost a fortune and they run the risk of losing customers."

"Within the next decade, we could very likely see a Wall Street hack that is big and bad enough to cause our next financial crisis."

"A lot companies just focus on firewalls and keeping hackers out but not what to do if and when a hack breaks through"

"Two changes on Wall Street could make a big difference: 1) making sure that third-party vendors that banks do business with are up-to-snuff; 2) outdated password systems need an upgrade."

BANGKO SENTRAL NG PILIPINAS

"It is no longer an IT problem, it's a top issue."

Small Banks, Vulnerable to Cyber Attacks?

timeinc.net

FORTUNE

Subscribe

TECH

Hackers Prey on Smaller Firms as Big Banks Harden Security

JEFF JOHN ROBERTS
JUN 23, 2016 7:30 AM EDT

BANKVAULT Cyber Security

How Small Banks Are at Risk from Cyber Criminals

Posted 31 MAR, 2016 by Graeme Speak

Every other few weeks, we hear of an online attack targeting the big banks. It is easy to be mistaken to conclude that the criminals solely attack the big international banks. The truth of the matter is that the smaller banks are more at risk at being

DIGITAL TRANSFORMATION & CYBERSECURITY LANDSCAPE

Malware
Ransomware

Advanced Persistent Threats
DDoS Attacks

ATM
Malware/ATM
Host **Spoofing**
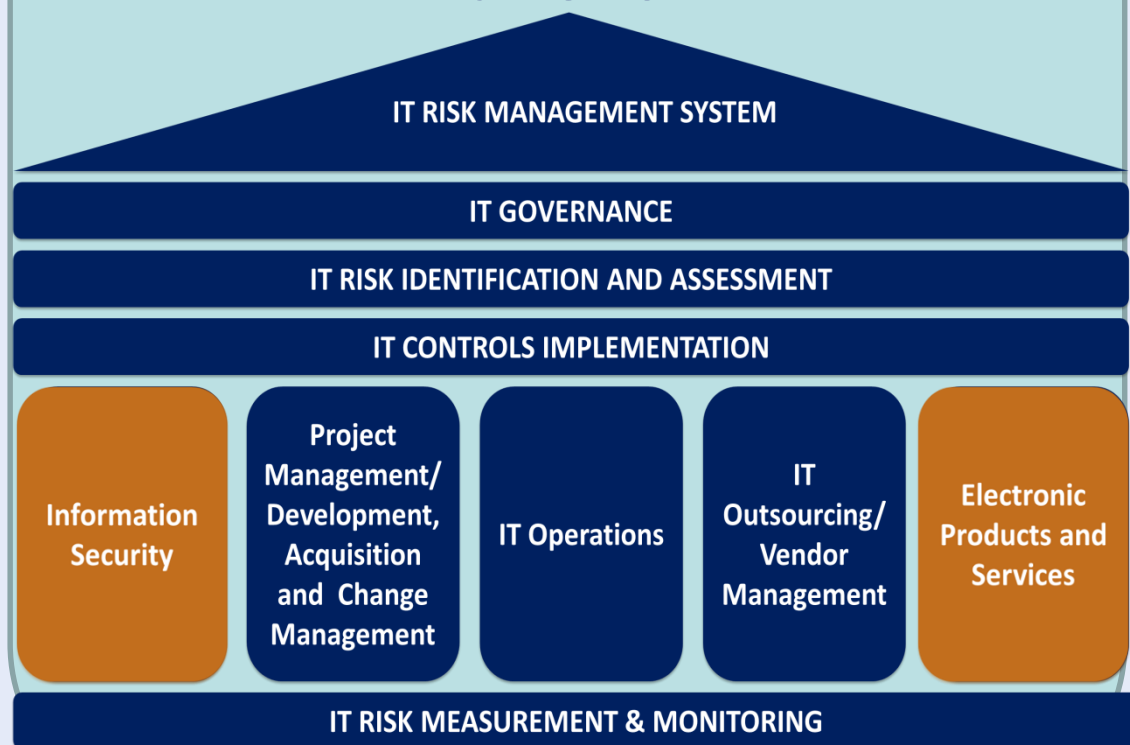CNP Fraud

Phishing
Spearphishing

BSP REGULATORY FRAMEWORK

Circular No. 808 s. 2013 ITRM Framework

IT RISK MANAGEMENT SYSTEM

IT GOVERNANCE

IT RISK IDENTIFICATION AND ASSESSMENT

IT CONTROLS IMPLEMENTATION

Information Security	Project Management/ Development, Acquisition and Change Management	IT Operations	IT Outsourcing/ Vendor Management	Electronic Products and Services

IT RISK MEASUREMENT & MONITORING

Subsection X701.1 – Prescribes minimum pre-conditions before banks can engage in e-banking services

Public Advisories and Memoranda– To increase awareness on emerging threats

IT Examination | Licensing | IT Policy Development

BSP Regulatory Framework

Recent Policy Issuances

BSP Cir. 958 dtd. 25 April 2017 – Multi-Factor Authentication Techniques

BSP Cir. 951 dtd. 20 Mar 2017 – Business Continuity Mgt. Guidelines

BSP Cir. 949 dtd. 15 Mar 2017 – Social Media Risk Mgt. Guidelines

Various MAAB - covering EMV Migration, Phishing and Fraudulent Websites and Ransomware and other malware attacks, among others

BSP REGULATORY FRAMEWORK

Enhanced Information Security Guidelines

Key improvements:

➢ Alignment with NIST, FFIEC and CPMI standards/frameworks

➢ Definition of cybersecurity risk management controls and supervisory expectations

➢ Requirement for behavior-based threat detection, threat intelligence and collaboration

IT Profile

COMPLEX

- Uses technology extensively in supporting mission-critical business processes and delivering financial products and services
- Has ubiquitous branch network and offers a wide array of digital/electronic financial products and services
- Highly interconnected with external third party stakeholders and actively participates in e-payment systems and networks
- Business strategies are largely anchored on IT platforms and digital innovation
- Aggressively utilizing/exploring emerging technologies

IT PROFILE

MODERATE

- Uses technology to some extent, but not as aggressively as complex institutions
- Branch network, IT organization and structure, and extent of IT projects are relatively less significant than complex institutions
- IT applications and systems are integrated but primarily support traditional banking products and services
- Offers basic digital/electronic products and services, such as ATM terminals/card-based products, to a limited number of clients

BANGKO SENTRAL NG PILIPINAS

IT PROFILE

SIMPLE

- Has very limited use of technology with minimal interconnectivity to its clients and other institutions
- Branch network or geographic presence is confined to a specific locality
- IT applications and systems are stand-alone or are not fully integrated and e-banking products and services are rarely offered
- Has few IT personnel and customer base

Cyber Governance

Strong Leadership

Tone at the Top

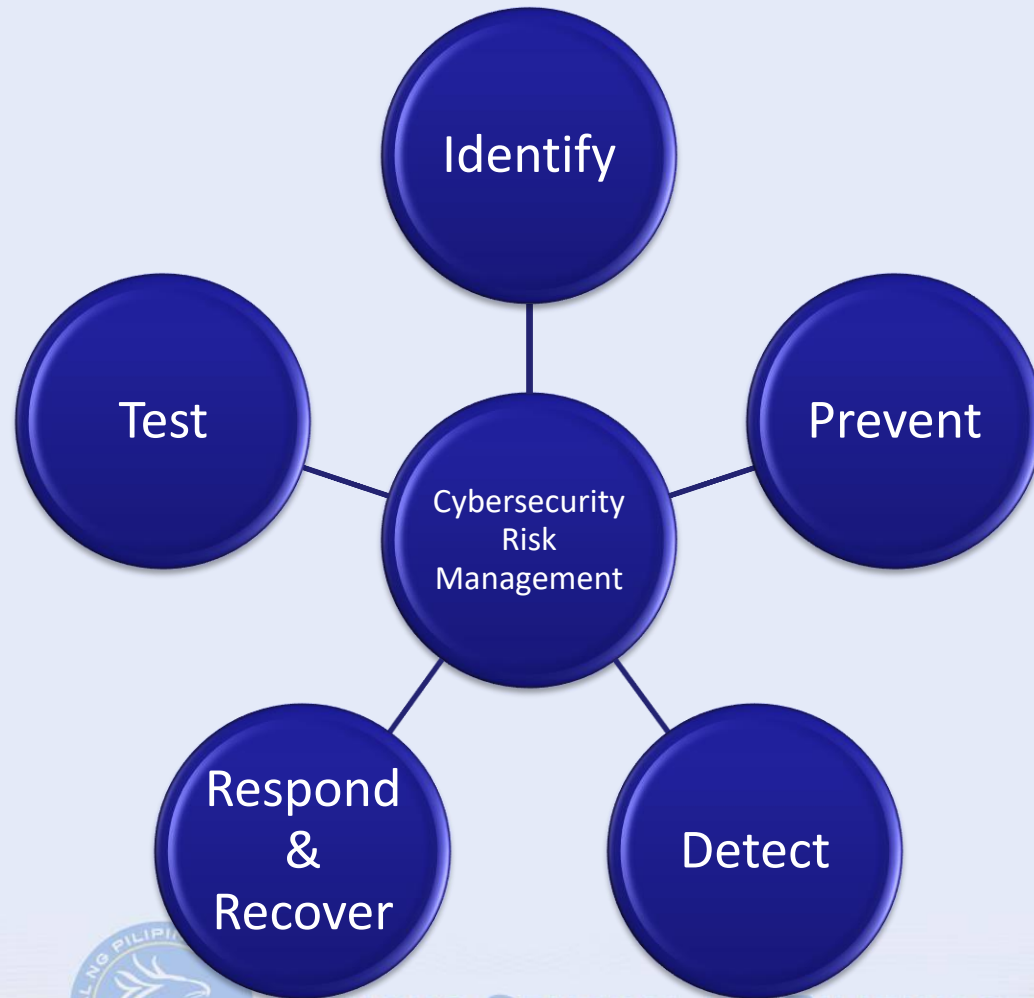**Cybersecurity Culture**

CS RISK MANAGEMENT PROCESS

CS Risk Management Process – Threat Intelligence & Collaboration

- Situational awareness and threat monitoring
- Security Operations Center (SOC)
- Emerging technologies and innovations
- Information sharing and collaboration

Baseline Requirements for Simple BSFIs

- IS governance process
- Inventory of information assets
- Information security program (physical, administrative and technical controls)
- Perimeter security and end-point security
- User access rights management
- Understanding of baseline performance/ behaviour
- Business continuity plan
- Security audits and compliance checks

BSP's Cybersecurity Roadmap

Expansion of e-Services (Products and Usage)

Emergence of New and Evolving Risks

Technological Advances and Innovation

Increasing Sophistication of Threats

Continuously enhance BSP regulatory framework vis-à-vis emerging cyberthreats

Undertake industry-wide initiatives to promote financial system resilience

Adopt proactive supervisory monitoring and oversight

#secure #vigilant #resilient

SALAMAT PO!