WORLD BANK GROUP
Information and Technology Solutions

Cybersecurity
Risks and Opportunities

Syed Mehdi Hassan, World Bank
Doha, State of Qatar
5 November 2017

Agenda

- Key Cybersecurity Risks in Financial Sector
- Recent Cybersecurity Events
- Cybersecurity Landscape
- Threats and Vulnerabilities
- Risks and Opportunities
- Vulnerabilities
- Using Principles
- World Bank Technical Assistance Programs

Key Cybersecurity Risks in the Financial Sector

- **Direct Financial Loss:** Monetary loss through cyber crimes

- **Indirect Financial Loss:** Cost of recovery/remediation, Loss through market share shrinkage, reputation damage, regulatory fines, etc.

- **Client Data Loss**: Loss or unauthorized disclosure of client Information

- **Service Unavailability:** service level agreements and expectations set with stakeholders may not be met (indirectly revenue may be lost and penalties imposed)

- **Money Laundering:** proceeds of crime are transformed into legitimate money or other assets.)

- **Fraud:** Losses due to malicious acts intended to swindle or misappropriate property

Recent Cybersecurity Events

Central Bank of Bangladesh heist attempt to steal $951 million through fraudulent Swift transactions

Bangladesh Bank

Feb. 2016

Deloitte.

Compromised email system. Several gigabytes of data exfiltrated

Sept. 2017

Personal information associated with an estimated 3 billion Yahoo! user accounts was compromised

YAHOO!

Dec. 2016

EQUIFAX

Breach exposed sensitive data for 143 million US customers

Sep. 2017

WannaCry

Over 45,000 ransomware attacks reported in over 100 countries around the world

May 2017

2016 DEMOCRATIC NATIONAL CONVENTION

State sponsored hacker group infiltrated the systems of the Democratic National Convention

Jun. 2016

Recent Cybersecurity Events – Key Lessons

Red indicates countries impacted by WannaCry

Key Lessons:

- **Brilliant on the Basics** - Install the latest patches, upgrade systems before they are out of vendor support.
- **Manage vulnerabilities** - Have adequate processes to detect vulnerabilities and missing security patches. Equifax ordered patch deployment back in March, yet failed to detect missing patches.
- **Strengthen security monitoring and threat detection** - The attacker gained initial access to sensitive data on May 13, 2017. Equifax first observed suspicious activity on July 29.
- **Conduct phishing exercises** – Phishing emails were the primary delivery method for WannaCry.

The Changing Cybersecurity Landscape

- Cybersecurity is not a problem that can "be fixed", but rather a **persistent issue** requiring a series of dynamic trade-off decisions
- Perfect protection is difficult to achieve. Focus on **detection and response** to reduce dwell times of threats and the potential damage when breaches inevitably occur
- Focus cannot be solely technology-driven, but must be **augmented by changes in user behavior** driven by a corporate security culture
- Cybersecurity is not an IT-only issue, but an **enterprise-wide issue** requiring a risk management approach

Information Security Threats

External Threats

- Organized Crime
- Hacktivist Group
- State or Business Sponsored Entity

Internal Threats

- Careless/Unaware User
- Malicious Insider

- Destructive attacks are evolving i.e. NotPetya Ransomware network worm designed to destroy data
- Data manipulation and data integrity attacks are increasing, some with objective to create “fake” information to support propaganda
- Proliferation of insecure IoT devices leads to more Distributed Denial of Service (DDoS) attacks
- Third-party breaches exposing staff’s sensitive data
- Business email compromises where phishing emails were targeted at senior management, staff, and central banks
- Ransomware attacks are becoming more targeted as it is a lucrative business model for cyber criminals
- Nation state actors are launching more sophisticated attacks

Attack Patterns

- Crimeware
- Cyber-Espionage
- Denial of Service
- Insider and Privilege Misuse
- Errors
- Web Application Attacks
- Business Email Compromises (CEO Fraud)

Risks and Opportunities

	Strategic Elements	Potential Risks	Opportunities
	**Cloud Adoption**	• Unauthorized disclosure of data due to commingled environments • Loss of governance and control • Shadow adoption	• Increased business resiliency • Leverage vendor's security capabilities • Faster time to market • Cost efficient solution to improve country office performance • Embed cloud risk management into ITS Risk Management • Availability of innovative solutions
	**Expanded usage of mobile devices**	• Loss or theft of sensitive information • Geo-tracking of employees and clients	• Better user experience • Increased productivity • Location and device independence
	**Use of 3rd party services**	• Unavailability of core services • Unauthorized disclosure of data • Vendor lock-in	• Increased agility and flexibility in meeting business delivery needs • Optimize sourcing options

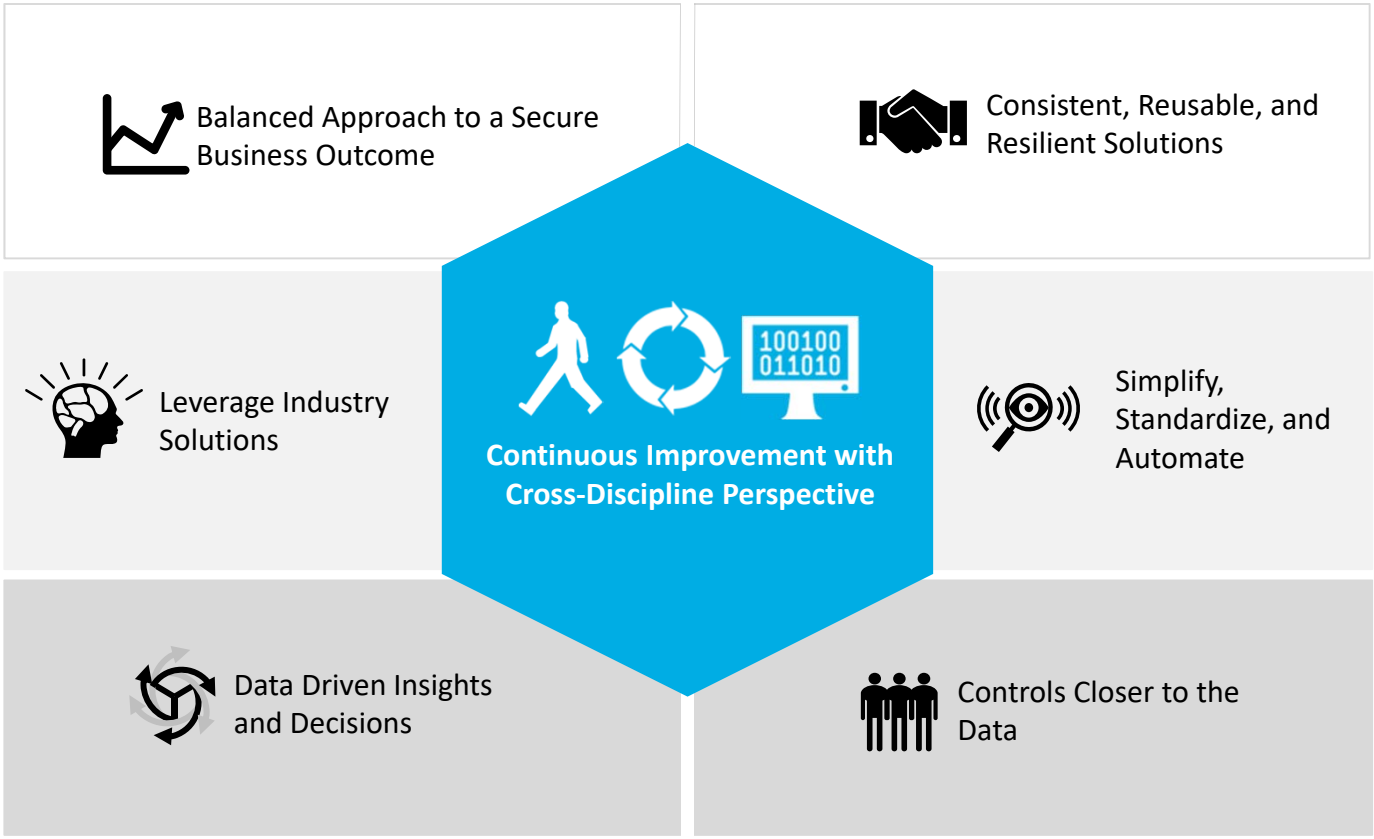
Vulnerabilities

- Maturing information security culture
- Fluctuating contingent workforce
- Accommodations for personal and consumer-based technology

- Emerging capability for identification and governance of critical information assets
- Inconsistent information classification
- Maturing data access, privacy protection and vendor management practices

- Evolving cloud and third party vendor landscape
- Complex IT infrastructure and delayed patching
- Potential weak controls and cybersecurity posture of associated partners and third parties

Using Principles to Guide the Program



World Bank Technical Assistance Programs

Given the increasing critical importance of Cybersecurity to the global financial stability, the World Bank has setup a cross functional team that provides technical assistance to member states in the following key areas:

- Developing regulatory and supervisory practices on cybersecurity in the Financial Sector
- Conducting Cyber Crisis Simulation Exercises
- Assistance in preparing National Cyber Security Strategy Guidelines
- Tools and capacity building to combat cybercrime in emerging economies (World Bank Toolkit to Combat Cyber Crime)

Thank you