

# Agenda

- 1. Do You Need to Be Concerned?**
- 2. What organizations can do to better protect**
- 3. What you can do personally to better protect**
- 4. Questions**



*Do You Need to Be Concerned?*

# Video

What is Your Password?

# Understanding the threat landscape

**ALL COMPANIES ARE ALL AT RISK.  
NO MATTER THE SIZE OR INDUSTRY.**



Attacker gained access to 250,000 user records and passwords



Chinese attackers took control of 53 User workstations and stole data



40 Million credit cards & 70 Million customer records stolen. CIO and CISO resigned



Hackers captured user accounts, email addresses, phone numbers of 145 million users



80 Million Customer Records Stolen



53 Million eMail addresses stolen. Stolen account information obtained by a third-party to gain access

# Understanding the threat landscape

**15%**

INCREASE IN  
THREAT  
ACTIVITY IN  
THE  
FINANCIAL  
SERVICES  
INDUSTRY

**33%**

OF BREACHES  
WERE DISCOVERED  
INTERNALLY  
DOWN FROM  
37% IN 2012

**9**

**MILLION+**  
PEOPLE EXPERIENCE  
IDENTITY THEFT EVERY  
YEAR

**2.5**

**BILLION**  
RECORDS  
COMPROMISED  
OVER THE PAST  
FIVE YEARS

**8**

**MONTHS**  
IS THE AVERAGE TIME AN  
ADVANCED THREAT GOES  
UNDETECTED ON A  
VICTIM'S NETWORK

**1 IN 5**

ORGANIZATIONS  
HAVE BEEN  
ATTACKED

**62%**

INCREASE  
IN BREACHES

# Understanding the threat landscape

- **Organized Crime, Hactivists, Nation State, Industrial Espionage, Insider Threat, Careless Employees all pose Threats to the Financial Services sector**

- **Introduction to new technologies such as Mobile, Cloud Computing, Data Analytics are introducing new security challenges**

**The Threat is Intensifying**

**Technology Landscape is Changing Fast**

**Vulnerabilities and Attack Vectors are Expanding**

**Business Partners and Customers Expect Security & Trust**

- **There are expanding methods and portals where weaknesses are exposed including, E-Mail / Web, Web User Interface, Identity Compromise, Physical Access & Social Engineering**

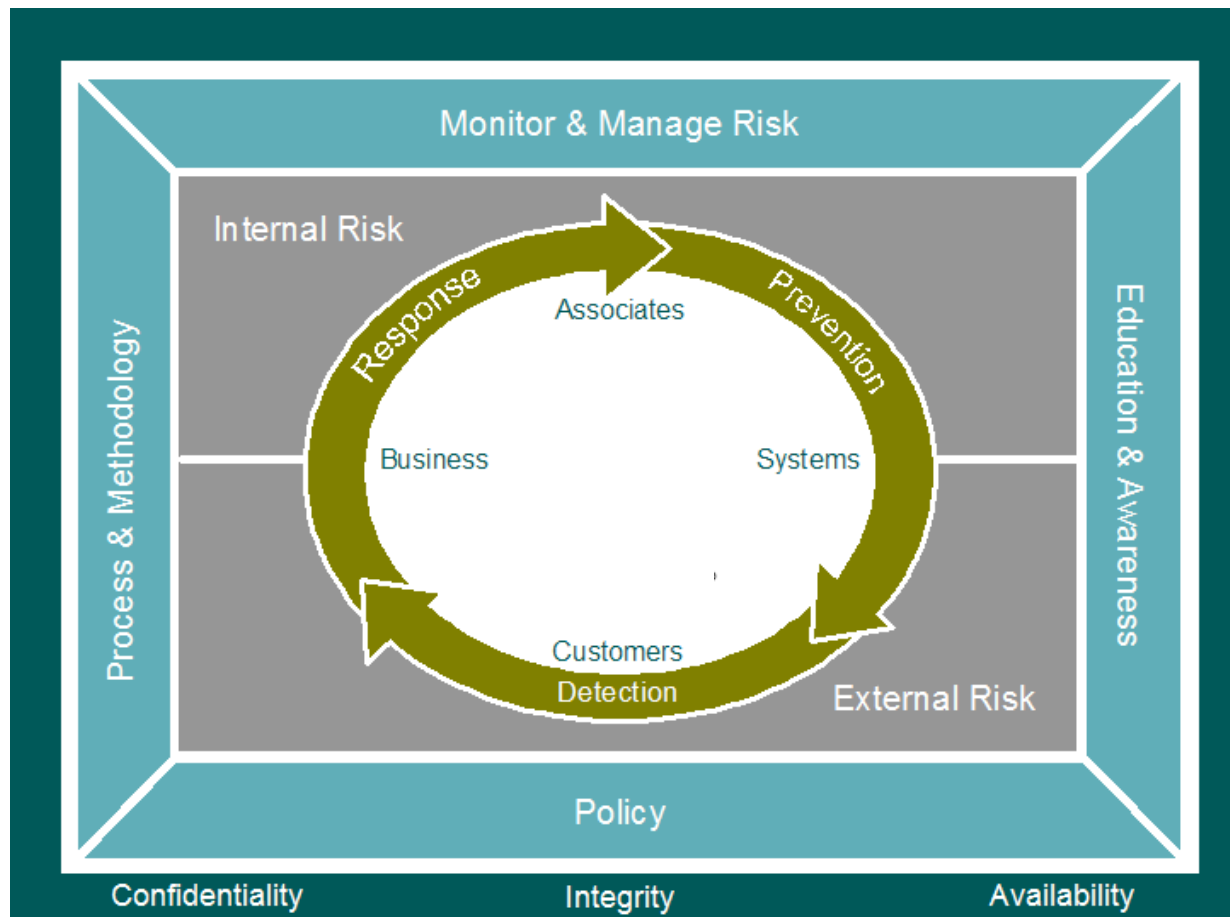
- **Participants and Customers are asking for this functionality to better protect their information**



*What organizations can do to  
better protect?*

# A Risk Management Framework

## Aspects of the Risk Management Cycle & Components





# Security Management



Will Look for  
Vulnerabilities  
and Weakness  
at each Layer

New  
System  
Developme  
nt

Legacy  
Systems

Highly  
Regulated  
Systems  
(SEC,  
FINRA, etc)

Test  
Systems  
with  
Confidentia  
l Data

Shadow IT  
Systems

Mainframe,  
Mini,  
Workstatio  
n Systems

Internet  
Systems

Human & Process Layer

Application Layer

Database Layer

Platform Layer (Operating system)

Network Layer

Physical Layer

***Data (Confidential Information)***

# Defense in Depth

## *(Area's for Preventative Care)*

- **Physical Layer** - Locked Computer Rooms / Data Center, Building Security, Unsecure Laptops, Closets, etc.
- **Network Layer** - Network Architecture, Firewall, DMZ's, Router Configurations, Filters, etc.
- **Platform Layer** - O/S Patches, Templates, Configuration, etc.
- **Database Layer** (e.g., Oracle, SQL) - Patches, Templates, Configuration, etc.
- **Application Layer** - Authentication and Authorization Engines/Architecture, Secure Coding Practices, OWASP Top 10 (SQL Injection, Cross Site Scripting, Secure eMail, Optium etc.)
- **Process** - Social Engineering, Phishing, Provisioning Processes, Account Management, Generic ID Management, Education & Awareness, Policy Management, Change Management, Segregation of Duties)

# Detection

## *(Area's for Detective Care)*

- **Physical Layer** - Audits, Interview, Visual Observations
- **Network Layer** – Vulnerability Scanning Tools (nessus), Attack and Penetration Testing's, Intrusion Detection, Intrusion Prevention
- **Platform Layer** – Vulnerability Scanning Tools
- **Database Layer** – Vulnerability Scanning Tools, Database security tools; Inspection's
- **Application Layer** – Vulnerability Scanning Tools, Password Crackers, etc.
- **Process** Access Review Tools, Social Engineering Testing, Audits, Open Risk & Issue Management
- **Across Multiple Layers** – Data Loss Prevention (DLP), Forensic Capabilities (e.g., outsourcing), Anti-Virus, Advance Persistent Threat detection

# It should be “Everyone’s” Job

## Baking Security into the Practitioners Role - Notes

- Define the What and the How.....
- Re-use/leverage existing awareness and education documentation
- Conduct More Education and Awareness (E&A)
- Establish targeted E&A to be role specific
- Establish Roles & Responsibilities document (by role)
- Establish Decision Rights
- Establish Consequences for non-compliance
- Establish a checklist of controls for Asset Owners
- Establish Self audit process (including validation)
- Establish process to revisit based on risk
- Handbook for the Role of the asset owner



*What Can You Do to Better Protect  
Yourself and Your Sensitive Data?*

# Over Sharing and Social Media Tips

- ✓ **Consider what you post**
- ✓ **Control visibility and privacy**
- ✓ **Routinely check your settings**
- ✓ **Respond to a breach**



# Ways to Protect

- ✓ Turn on WPA2
- ✓ Make passwords long and strong
- ✓ Unique account, unique password
- ✓ Keep a clean machine
- ✓ Automate software updates
- ✓ Admin user account only to complete a specific task
- ✓ Consider the information you post on social sites
- ✓ Enable a firewall (Personal Firewall)
- ✓ Limit use of administrator accounts
- ✓ Protect your \$\$
- ✓ Don't be tricked into opening an attachment or providing confidential information about yourself
- ✓ Never provide your user ID & password via a clicked-on link from an email or text
- ✓ When in doubt, throw it out

# Recognize & Avoid Phishing

## Red Flags



- ✓ Check the sender
- ✓ Dear Customer
- ✓ Bad spelling and grammar
- ✓ Urgent requests
- ✓ Be careful with website links
- ✓ Be suspicious of attachments
- ✓ Requests for sensitive information
- ✓ Sound too good to be true?



# Questions

M. Travis Michalak

Associate Vice President

Nationwide Financial – Information Risk Management

[michalm@nationwide.com](mailto:michalm@nationwide.com)

614-677-6809

1 Nationwide Plaza

3-17-202

Columbus OH 43215



## Thank You!