Information Security in Operational Risk Part I

Presented by:
Eric Holmquist
Managing Director, ERM Practice
Accume Partners

ABOUT RMA

Founded in 1914, The Risk Management Association is a not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, and operational risk.

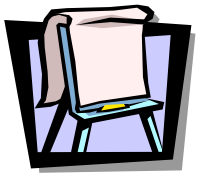
Headquartered in Philadelphia, Pennsylvania, RMA has 2,500 institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by more than 16,000 risk management professionals who are chapter members in financial centers throughout North America, Europe, and Asia/Pacific.

ABOUT ACCUME PARTNERS

- Founded in 1994
- Largest independent provider of internal audit, regulatory compliance, enterprise risk management and technology risk management services to the financial industry
- Services span:
  - Governance, Risk Management and Compliance
  - Operations and Process Improvement
  - Technology Risk Management
- Regional offices in NY, NJ, CT, MA, PA, MD and NC
- Our clients are in the following industries:
  - Financial Institutions (85%)
  - Insurance (5%)
  - Commercial (5%)
  - Education (5%)

INFORMATION SECURITY

Agenda



- What's new?
- Defining is a risk-based approach to information security
- The information security program
- Assessing IS risk
- Summary and final thoughts

INFORMATION SECURITY

From the 2013 Verizon Business Data Breach Investigations Report:

- 37% of the breaches affected financial organizations
- 92% perpetrated by outsiders (but this includes recent terminations)
- 76% of network intrusions exploited weak or stolen credentials
- 52% utilized some form of hacking
- 78% of intrusions rated as low difficulty
- 69% of the breaches were identified by a third party
- 9% were spotted by customers
- 66% of the breaches took months or years to discover

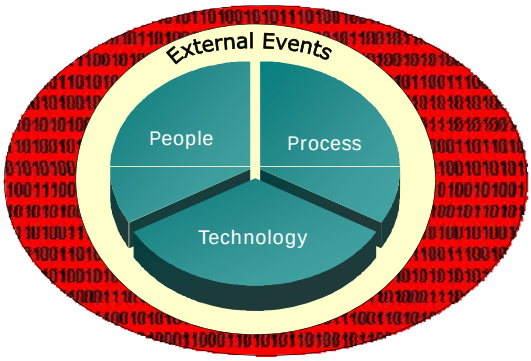
INFORMATION SECURITY

From the 2014 Verizon Business Data Breach Investigations Report:

- 34% of the breaches with confirmed data loss affected the finance industry (followed by public 13%, retail 10% and accommodation 10%)
- 75% can be described by 3 specific attack patterns (financial services)
- Motives remain #1 financial, #2 espionage and #3 fun/ideology
- Use of stolen credentials the top attack method
- Hacks to user devices somewhat flat
- Criminals are getting faster
- Discovery is not

WHERE DO WE START?

Information security must be approached as a business issue not a technology issue. Once we agree on this, then we can consider using risk management practices.



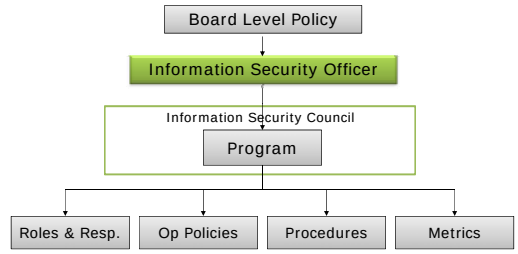
KEYS TO INFORMATION SECURITY GOVERNANCE

- InfoSec can't be managed to 80/20 rule
- You can't start at controls first
- If you can't answer these 4 questions, you don't have an information security program:
  - Where is my data?
  - What is my exposure?
  - What are my key controls?
  - What is my residual risk?

TAKING A RISK-BASED APPROACH MEANS…

- Agreement on risk appetite and tolerance
- Cross functional governance
- Comprehensive risk assessment methods
- Dynamic risk measurement methods
- Ownership and accountability
- Effective communication
- Ensuring ability to quickly respond
- Meaningful reporting mechanisms

INFORMATION SECURITY GOVERNANCE



ESTABLISHING RISK TOLERANCE

- Fact: Senior management always says they have a “very low” risk appetite. Actually, you don’t.
- Must have realistic and comprehensive risk assessment tools to understand the risk profile.
- Requires deep, honest discussions with a lot of people to fully understand the risk.
- In practice, this area scares people to the point of not being able to face it head on. That model will never successfully address risk tolerance.

INFORMATION SECURITY POLICY

- Board level policy
- Establishes issue as business risk
- Defines the role of the ISO or CISO
- Sets mandates for program
- Establishes program expectations
- Defines board notification provisions
- Not detailed in program specifics
- Using Operating Policies for specifics

INFORMATION SECURITY OFFICER

WRONG!

INFORMATION SECURITY OFFICER

- Senior, if not executive level position
- Preferably not in IT
  - Better in Risk Management
- Must have senior access
- Must have extraordinary interpersonal and communication skills (written and verbal)
- Must have both business and some technical skills
- Most important role will probably be as translator

INFORMATION SECURITY PROGRAM

- Regulatory requirement
- Supports issue as business risk
- Documents major components
- Eliminates unspoken assumptions
- Sets clear responsibilities
- Defines risk-based approach
- Establishes training curriculum
- Supported with operating policies

INFORMATION SECURITY COUNCIL

- Must have authority to set policy
- Make it cross-disciplinary
- Get senior participation
- Make it visible
- Make it safe
- Honesty is critical

ENGAGING SENIOR MANAGEMENT

- Starts with education and awareness
- Balance risk information with risk treatment
- Once educated, solicit active input
- Language is key!!!!

THE ROLE OF IT

- IT is one part of the conversation, but a critical one
- Lives a dilemma between serving and controlling
- Must come to an agreement on risk tolerance level
- Guardians of systems, not content
- SMEs of "What could go wrong?"
- Use IS Council to set policies
- Strive for a risk aware culture
- Don't assume anything

THE ROLE OF IT

- Independent vulnerability studies are critical
- At least yearly, more often if needed
- Patch management program remains one of the most critical areas on which to focus
- Credentials really do matter
- Bring Your Own Device (BYOD), must have:
  - A "Right to wipe" acknowledgement
  - Acceptable use policy
  - Encryption
- Change control process is really key
- Document everything

CULTURE - BUILDING A BIG ARMY

- Training is your single best IS investment
- Create a culture of cooperation
- Build social intolerance to data exposure
- Make it everyone's responsibility
- Make disclosure safe
- Don't underestimate instincts
- Reward creativity
- Make it positive, not negative

INFORMATION SECURITY TRAINING

- Realize we are training three different groups
- Program overview is a good thing
- Context is very important
- Educate on the real risk
- Clear do's and don'ts
- Make it ongoing
- Make it interesting!

ROLE OF REGULATIONS AND STANDARDS

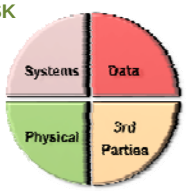
(e.g. Sox, ISO, FFIEC, GLBA, PCI-DSS, etc.)

- All guidance is risk-based
- Most focus on assumptions and managing change
- Not program design specs!
- Focus first on risk aspects
- Use specific provisions as tests
- Leverage compliance process

ASSESSING INFO SECURITY RISK

- Focus must be on risk, not just controls
- Everything starts with the risk assessment
- Manage to assessed risk, not perceived risk
- Have to understand inherent vs. residual risk
- Insiders are probably more of a threat than outsiders, and their impact is much bigger
- Ability to respond quickly and effectively is critical – Time is not on your side!

ASSESSING INFO SECURITY RISK



- Inventories are critical
- Approach 4 ways:
  - Information systems
  - Electronic data
  - Physical files
  - Third parties
- Focus on accountability
- A good assessment should always start from what you know.. that you know.. that you know
- Use self-assessments vs. loss data or scenarios
- The worst possible answer to assessing information security risk is…

RISK QUANTIFICATION

- Risk is quantified in four categories:
  - What's at risk?
    - Customer, corporate, third-party
  - What would be the impact?
    - Financial, operational, regulatory and reputation
  - What could be the source?
    - Internal, external and natural disaster
  - What can we mitigate?
    - Prevention, monitoring and recovery

ASSESSING INFO SECURITY RISK

- Should IS be assessed separately or as part of all individual operational risk assessments?
- Could be approached either way, with pro's and con's to each.
- However, regardless, you need to end up with an overall assessment of risk.
- Note that an information *security* risk assessment is something different than an information *technology* risk assessment.

PRESENTATION SUMMARY

- Everything starts with strategy
- Focus on risk awareness (culture)
- Training is absolutely critical
- Assessing risk means involving a lot of people
- You're not focused enough on internal risk
- You need more discussion about residual risk
- Establish agreement on risk tolerance
- Honesty and transparency are key

Enterprise Risk · Credit Risk · Market Risk · **Operational Risk** · Regulatory Compliance · Securities Lending

Information Security In Operational Risk Part I

Presented by:
Eric Holmquist
Managing Director, ERM Practice
Accume Partners
eholmquist@accumepartners.com

JOIN. **ENGAGE.** LEAD.