Information Security in Operational Risk Part II

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.

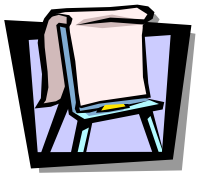
Headquartered in Philadelphia, Pennsylvania, RMA has 2,500 institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by more than 16,000 risk management professionals who are chapter members in financial centers throughout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



- Prior session recap
- Data management
- Change management
- Data breach response
- Monitoring and reporting
- Topical application areas
- Summary and final thoughts

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

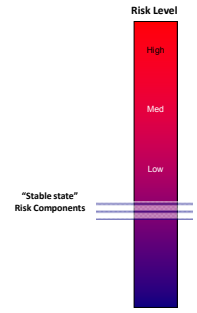
SUMMARY RECAP

- Define risk appetite
- Information security policy and program
- Information Security Officer
- Information Security Council
- Role of IT
- Build the culture
- Structure for assessing risk

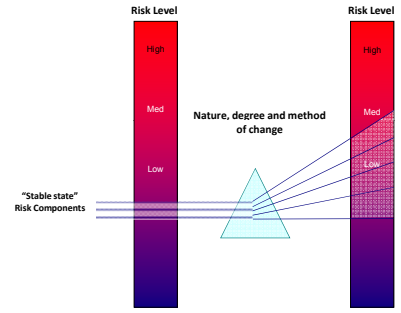
DATA MANAGEMENT

- Probably your highest area of residual risk
- You can't manage risk if you don't know exactly where your data is…..period!
- Beyond that…
  - Who, what, when, where, why and how
- Acquiring data access should be difficult
- Leverage monitoring technology
- View data like cash

THE "PRISM" EFFECT OF CHANGE



THE "PRISM" EFFECT OF CHANGE



CHANGE MANAGEMENT

- Risk management begins with strategy
- Requires understanding assumptions and agreed upon risk tolerance levels
- Critical to have both IT & business input
- In this context, expand the analysis to confidentiality, availability and integrity
- Remember, all operational risk failures are attributable to a change of some sort

DATA BREACH RESPONSE PROGRAM

- Establish a primary and secondary coordinator
- Clear roles and responsibilities
- Link to incident response program
- Must have a first-day checklist
- Notification list and procedures
- Staff training is critical
- Data breach exercise!

MONITORING AND REPORTING

- Information security by nature defies M&R
- There is a limited amount we can monitor and monitoring systems create a lot of noise
  - However, it is critical and data trends can be meaningful
- Tie into KRI program – what *can* we track?
- The real value may be in the visibility
- Reporting must be timely, clear, root-cause focused and actionable
- Some of this stuff really is interesting

CLOUD SERVICE PROVIDERS

- This model is not at all new, just the technology
- Mirror your internal standards
- Must be very clear on:
  - Fault tolerance
  - Data proximity
  - Data location
  - Service levels
- Tech specs matter
- Regulatory focus

Source: Techiestate.com

VENDOR MANAGEMENT

- Proper oversight and due diligence is not optional, it's mandatory:
  - Where's the data?
  - Who has access?
  - How are you protecting it?
  - Use documentation (SOC report, SIG, etc.), but never stop asking hard questions
- For Internet Banking vendors, how will they stop a DDOS attack?
- What are your breach response SLA's?

DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

- Increasing in frequency
- May be one of two types:
  - Flooding site
  - Direct server attack
- May be a smokescreen for other activity
- Must address with your Internet Banking vendor
- If self-hosting:
  - Talk with your Internet Service Provider
  - Explore availability appliances
- Mobile may be a good alternate channel

MOBILE BANKING / MOBILE DEVICES

- Still more unknowns than known's
- Increased fraud?
- No "remember me" options
- Ensure aggressive timeout requirements
- Clear terms and conditions are critical
- Customer awareness

OTHER TRENDS AND ISSUES

- **Phishing** is an ongoing threat
- **Social Engineering**
- **Configuration Management**
- **Advanced Persistent Threats** (ATP)
  - Known foreign sponsored groups
  - Long-term, sophisticated attacks
  - May be low-and-slow vs. brute force
- **Patches** remain your most critical protection
- Comprehensive risk management is more critical than ever!

OTHER RESOURCES

- http://www.verizonenterprise.com/
- http://www.darkreading.com/
- http://www.ponemon.org/
- http://www.searchsecurity.com/
- http://msisac.cisecurity.org/
- http://www.sans.org/
- https://cloudsecurityalliance.org/
- https://sharedassessments.org/

PRESENTATION SUMMARY

- Risk management always comes down to assumptions
- Cross disciplinary involvement is truly key
- As we become more technology dependent, our risks will increase
- We simply have to know what our risk profile is
- Managing change is critical to this area of risk
- How you respond to an event is just as important as how you've prevent it
- As always, it's all about awareness, accountability and actionability

Information Security In Operational Risk Part II

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