Data Security Breach
How to Respond
About ERM

mission
To protect individuals, organizations and society through comprehensive risk management.

vision
Worldwide leader and trusted advisor in Enterprise Risk Management.

values
Ethics. Do the right thing.
Trust. Provide transparency and protection.
Excellence. Provide the highest quality.
Service. Help clients, employees and society.
Can-Do Attitude. Face and overcome challenges.
Passion. Love what we do.
About The Speaker

- Information Security Director at ERM
- CISSP, CISA, CRISC, PCIP, PCI-QSA

Core Experience:
- Information Assurance
- Computer Forensics
- Penetration Testing
- Regulatory Compliance and Standards
- Technical Security Assessment
- Social Engineering
Agenda

- What is a Data Security Breach
- Breach Management Plan
  - Containment and Recovery
  - Risk Assessment
  - Notification of Breach
  - Evaluation and Response
- Some Statistics
- Conclusion
What is a Data Breach

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
Examples of Sensitive Data

- Name
- Address
- SSN
- Telephone Number
- Driver’s License Number
- Account Number
- PIN
- Email Address
- Password
- Student education records
- Other personal Information
Security Data Breach

Don’t Panic !!!
Breach Management Plan

- Containment and Recovery
- Risk Assessment
- Notification of the Breach
- Evaluation and Response
Containment and Recovery

- **The Goal:** limit the extent of the attack and thus the potential damage or loss.
- Determine who should lead the investigation.
- Determine the scope of the breach.
- Establish who needs to be aware of the situation.
- Determine whether there is something that you could recover.
- Define the response strategy.
Appropriate Strategy

- **Strategy Goal:** Limit the extent of the potential damage to and theft of resources.
- Need for evidence preservation.
- Service availability.
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy.
- Duration of the solution.
Containment and Recovery

- Document details, conversations and actions.
- Evidence Gathering
  - Chain of custody
  - Preserve the evidence
- Follow notification escalation procedures.
- Apply changes to systems to control the attack.
Containment and Recovery

- Putting compromised resources back in service.
- Restore from a known good backup (before the compromise).
- Monitor closely for re-compromise.
Risk Assessment

- Determine what type of data is involved and its sensitivity.
- Determine how the data was protected during the incident.
- Analyze how many individuals were affected and who they are.
Risk Assessment

- Determine the harm that can come to those individuals.

- Determine the existence of wider consequences.

- If possible, determine what happened with the data.
Notification of Breach

- Obtain legal advice !!!!
- Contractual Agreement.
- The notification will help the individual.
- Number of people affected.
- Who, What, and How.
- Notify third parties (Police, Vendors, Insurers).
- Federal and State laws and regulations.
- Consider the dangers of ‘over notifying’.
Evaluation and Response

Some questions to be answered:

- How well did staff and management perform in dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- Were any steps or actions taken that might have inhibited the recovery?
- What corrective action can prevent similar incidents in the future?
- What would the staff and management do different the next time a similar incident occurs?
Some Statistics

Who’s perpetrating breaches?

92% perpetrated by outsiders

14% committed by insiders (+)

1% implicated business partners

7% involved multiple parties

19% attributed to state-affiliated actors (+)

Some Statistics

How do breaches occur?

- 52% used some form of hacking
- 76% of network intrusions exploited weak or stolen credentials
- 40% incorporated malware
- 35% involved physical attacks
- 29% leveraged social tactics
- 13% resulted from privilege misuse and abuse

Source: http://www.verizonenterprise.com/DBIR/2013/
Some Statistics

How do breaches occur?

- **52%** used some form of hacking
- **76%** of network intrusions exploited weak or stolen credentials
- **40%** incorporated malware
- **35%** involved physical attacks
- **29%** leveraged social tactics
- **13%** resulted from privilege misuse and abuse

Cost of Data Security Breach

Source: http://www.ponemon.org/

© 2013 Enterprise Risk Management, Inc.
Conclusion

- Document
- Develop policies and procedures
- Maintain the plan
- Learn from the common mistakes
Your go to advisors for all matters in information security.

800 S Douglas Road #940
Coral Gables, FL 33134

Phone: 305-447-6750
Email: info@emrisk.com

www.emrisk.com