Breach Response Planning:
Building the Better Mouse Trap
2014 was a terrible, horrible, no good, very bad year for cyber attacks. 2015 is shaping up to be just as bad...

Given the near-certainty that some form an attack or data breach will happen in your company, it makes sense to consider scenarios and plan for them when it happens

A data breach plan lays out the key steps and the key personnel to involve when a data breach happens
Security breaches are inevitable because determined attackers will always find a way through the gap.
Breach Response Objectives

Limit damage

Protect Brand Reputation

Collect and preserve evidence for prosecution of offenders

Collect data to demonstrate legal compliance

Collect data to prepare for litigation
Key Planning Areas
Management Response

Specifying incident handling procedures

Select a strategy for deciding on the course of action in a given situation

Procedures for communicating with organizational leadership and outside parties/law enforcement

Establishing employee expectations in conjunction with Human Resources (HR) policy and/or employee agreements
Management Response

Conducting regular reviews of the policy to include any necessary improvements

Ensure policy reflects up-to-date International, Federal, State, and local requirements

Procedures for emergency procurement and contracting

Requirements for notification of insurers

Contact rules and procedures for financial/bank accounts
Management Response

Identify the Executive Owner

Identify Stakeholders/Interested Parties

Identify the incident response team

Identifying a team manager who will be in charge of the incident response (with at least one other person designated to assume authority in the absence of the manager)

Assigning and establishing team roles and responsibilities, along with specifying access credentials

Consider creating a RACI or RASCI
Management Response

Figure 15. Functional areas that participate in the incident response planning process
More than one response permitted

- Legal: 85%
- Compliance: 70%
- Information technology: 70%
- Information security: 55%
- Human resources: 55%
- Finance & accounting: 54%
- Public relations: 53%
- CEO & board of directors: 47%
- Government or public affairs: 42%
- Internal audit: 40%
- Procurement: 30%
- Privacy office: 25%
- Security: 25%
- Risk management: 24%
- Logistics: 22%
- Marketing & communications: 22%
- Records management: 16%
- Sales: 9%

Source: Ponemon Institute LLC, *The Importance of Senior Executive Involvement in Breach Response*, October 2014
Technical Response

Identify capabilities, gaps, and experts
Determine what logs are available and log retention periods
Forensic capabilities
Vendor relationships
Incident Response Checklists
Technical Response

Data classification – privacy/regulated data
Data locations – processed, stored, transmitted
Logical and Physical Data Flow Diagrams
Network Diagrams
Legal Response

Identify legal, regulatory and contractual requirements

Breach notification requirements

What are the regulatory obligations and should law enforcement be notified?

Independent forensic investigation

Coordination with external parties, including law enforcement
Legal Response

Consider litigation matters that may arise, including:

a. Civil lawsuits instituted by affected persons against the company

b. Investigation of the company and/or specific employees by law enforcement authorities

c. Indemnification by third parties in the event that third parties are at fault for data security breach
The communication plan needs to address six critical audiences:

1. Internal teams (including Board and major investors),
2. Key partners and customers
3. Regulators and reporting agencies
4. Law enforcement
5. Impacted parties
6. Press, media and analysts
The communications plan should have a set of pre-approved web pages templates and phone scripts prepared along with frequently asked questions (FAQ’s) drafted and ready for posting.

Anticipate call volumes, take steps to minimize hold times and consider the need for multi-lingual support.

Consider a dedicated phone number for questions.
Communications Response

Key facts to include in external communications:

1. Incident description including what, how and when, (the more facts the better).
2. What type of data was lost or compromised?
3. Who was impacted, including estimate of the number and type of customers?
4. What action is the business taking to assist affected persons or organizations?
5. What steps are being put in place to help assure it will not happen again?
Key facts to include in external communications:

1. A statement that the situation is under control and it now safe to use your services?
2. What is being done to minimize the impact of identity theft for your customers?
3. Where can your customers go for information? (Contact info and toll free number)?
4. How will the organization keep customers informed and what are the next steps (critical in the early stages when all of the information may not be known)?
Training and Testing

Training

a. Train Executives

b. Train staff to be able to recognize and respond to breaches

Testing the Breach Response Plan
Assessing Your Capability Maturity Level

Figure 4. How mature is your organization’s data breach incident response?
1 = immature to 5 = mature

Source: Ponemon Institute
**Conclusions**

**Be prepared**

Always prepare for a breach in advance

Planning requires an interdisciplinary approach – not just IT

Document your environment and understand where sensitive data is stored, processed, or transmitted

Know your requirements for breach notification and evidence protection; do not underestimate the complexity of the forensic response

Executives and the staff should be trained on the plan and tested on a periodic basis
4. Internet Crime Complaint Center (IC3) http://www.ic3.gov/default.aspx
9. Incident Response Plan Template https://docs.google.com/a/berkeley.edu/document/d/18qMY5RSrYnfYfl6m1wV792xKz6qZ8VGUfgVbvfIk6gE/edit#
Questions? Comments?
I am happy to help you!

Bill Lisse
Bill.lisse@gmail.com