13 Challenges for Developing a Cybersecurity Incident Response Plan

November 12, 2014

Presented by: JoAnn Becker, MS, MBA, PMP

Agenda – Where are we going?

- Learning objectives
- Speaker information
- Acknowledge this Business Risk
- The Bakers Dozen of challenges
- Suggestions
- Q&A

Learning Objectives

Attendees will learn:

- Why having a cybersecurity incident response plan (IRP) must be part of ongoing operations for all organizations
- Why a cybersecurity response plan is so challenging – 13 points for the project manager (PMer) to address
- Suggestions for components of any organization's IRP

Speaker Information

JoAnn Becker, MS, MBA, PMP

Achieving Results from Change, Inc.
President

Cycle of Success Institute
Director of CPA Partnership Program and Senior Business Coach

JoAnn of ARC - JoAnn@AchievingResultsfromChange.com
(847) 682-5665
http://www.AchievingResultsfromChange.com
http://www.linkedin.com/in/joannbecker

Achieving Results from Change, Inc.

- 25+ years leading the strategy, design, development, implementation, marketing, and operations of change
- 15+ years managing all areas in IT (highly regulated banking)
- Leader of collaborative models for change - reduces the cost for all participants, trains people, and produces better outcomes
- Stakeholder expectation management/influence specialist
- Assess, design new processes, gain support, implement
- ETC: Educate, Teach, Coach – various seminars and courses
  - What Executives Need to Know about Cybersecurity Risks (3 hours)
  - How to Lead the Project to Develop a Cybersecurity Incident Response Plan (2 day workshop)
  - Executives Leading Change (private or group sessions)
  - Project Management for Non-IT People (1 day workshop)
  - Stakeholder Expectation Management (1 or 2 day workshop)
  - Leading Multi-Generations (1 or 2 day workshop)

Two Types of Organizations

Those who know they have been hacked

and

Those who don't know they have been hacked

Newest Business Risk

Cybersecurity is growing in complexity and number of attacks are increasing

- Breaches are there (those reported: Identity Theft Resource Center, July 8, 2014)
  - 181 in Medical/Healthcare for 1,877,660 records
  - 131 in Business for 6,378,168 records
  - 44 in Government/Military for 1,535,512 records
  - 26 in Educational for 1,113,461 records
  - 13 in Financial for 99,595
- Too many companies (per federal officials) are:
  - Ignorant, and
  - Unprepared

Current Issues

- Inability of many executives to understand their own technology employees…..
- Need to guard against breaches, but organizations must still have an effective cybersecurity IRP
- When organizations do have an IRP, most:
  - Do not operationalize it
  - Let their plan get out of date
  - Do not integrate it across business units, locations, countries
  - Permit their decision making to be based upon “tribal knowledge and existing relationships”
- With no IRP, how do organizations get insurance?
- No silver bullet – now or in future

Not an "IT" Project

The objective of a Cybersecurity Incident Respond Plan (IRP) is to develop how to manage actions after the incident to:

- Improve decision making
- Do better internal coordination (the attack is not just an IT issue)
- Limit damage – financial and others
- Increase confidence of external stakeholders
- Reduce recovery time
- Reduce recovery costs

Challenges: Bakers Dozen

The following are 13 challenges for the project manager (PMer) to handle when developing an enterprise (organization wide) plan to be followed when an organization becomes aware they have had a cybersecurity attack.

The IRP should describes what each and every individual must do (and not do) when an attack has been determined to have occurred – from the CEO down through to associates (with consideration also for consultants, suppliers, other stakeholders)

1. Participation

- The outcome of this project, the IRP, is to have instructions for every function, department, role, level, etc. in the organization.
- This means, the PMer must have a representative from each and all of these areas to participate in the project.

2. Diverse Stakeholders

Since the IRP is to include the entire organization, there will be input from all functions, departments, etc., including:

- Accounting
- Design – products/services
- Fabricate – products/services
- Finance
- HR
- Leadership
- Legal
- Marketing
- Physical facilities
- Planning
- Sales
- Technology

Plans for each must be integrated into **one** entire organization plan

3. Beyond the Skills of an IT PMer

The most needed competency for the project to produce an IRP is to be able to:

1. Identify all key stakeholders,
2. Ensure they are participating throughout the life of the project, and
3. Manage their expectations for success.

While Gantt and PERT charts, a schedule, and a budget are a part of the project, without the above competencies, this project will not succeed.

4. Knowledge of Technology

The Project Manager:

- Does not have to be a SME in technology.
- Does need to be familiar with and understand
  - Technology used by the organization, and
  - Technology for handling cybersecurity management, breaches, etc.
  - Be “bi-lingual”

5. Sponsorship

- An effective IRP (its development and execution when needed) relies upon executive sponsorship of this new item
- Assign an executive to have ongoing responsibility for:
  - The IRP
  - Integrating the efforts across business units and geographies
  - Responding to “what did the organization do to be prepared?”

6. Inform Board of Directors

Given today's world and what an attack can result in, the Board of Directors needs to be kept informed of:

1. How the organization is proceeding with their IRP,
2. Regular progress reports of its development, and
3. The results from regularly scheduled testing and updating of their IRP

7. Training for All

Successful implementation of an IRP needs:

- Training programs for all roles and levels to increase awareness of this business challenge and the new/changed IRP
- Regular training of all first-level participants of tasks in the plan, especially when updates are made

8. Test the Plan

Just as continuity of business (disaster recovery) drills are regularly practices, so too does the IRP. This confirms:

- People know what they are to do and not do
- External support agents are adequately informed and prepared
- Resources are available (people, tools, etc.)

9. Ongoing Updating of Plan

Change is now a constant for all organizations:

- Technology updates
- Buying and selling business units
- Business requirements (regulations, laws)
- Relocations
- People leave and are hired
- Other factors

10. Term of Employment

Legal documents that explain expectations and requirements for employment or being contracted (individuals or firms):

- Tasks for the IRP are followed
- Relevent information is reported as specified
- Other terms

11. Specialized Support

Areas in the IRP require SME not present in most organizations, and need to be contracted (monitored for expiration dates):

- Legal
- Security technology – in place, defense
- Security firm – the white knights
- Crisis management public relations firm
- Government: FBI, CIA, etc.

12. Ongoing Reporting

Regular reporting to management (executives, board of directors, etc.):

- Progress of IRP development
- Testing
- Security monitoring reports
- Updates
- Others

13. Hacker in Company?

While the number of hackers with inside knowledge (who have been instrumental in a hack, breach, etc.) has dropped significantly per current research, this is still a concern.

Suggestions

1. Education and training of the executive suite and board of directors – ASAP
2. Build a response program within your organization
3. Update plan for non-technology items (people who had key roles in the IRP leave the organization)
4. Update how major decisions are made, as needed
5. Identify how technology connections are made to vendors and other stakeholders
6. Continually update technology tools for security monitoring and detection
7. Learn shortfalls of most plans
8. Learn benefits of an effective plan

Suggestions

9. Learn components of a good plan
10. Learn guiding principles for successful plans
11. Do not wait for perfect or desire to have all information before taking action with execution of the plan with an incident
12. Plan to include how to engage with customers and other stakeholders
13. Provide a remedy to customers, consumers, patients, etc.
14. Communicate – communicate – communicate
15. Train – train – train
16. Practice/test – practice/test – practice/test
17. Buy breach insurance

ARC
Achieving Results from Change

Questions or Comments?

ARC
Achieving Results from Change