Be Prepared: Incident Response and Business Continuity Planning

Secure the Village
Cybersecurity Roundtable
June 2016

Stan Stahl, Ph.D.
President
Citadel Information Group
In preparing for battle I have always found that plans are useless, but planning is indispensable.

General Dwight Eisenhower
Incident Response and Business Continuity — What These Are

- Incident response management
  - Ensure proper management response to information security incident

- CIA Triad
  - Confidentiality
  - Integrity
  - Availability

- Business continuity
  - Planning, preparatory and related activities to ensure critical business functions
    - Continue to operate despite serious incidents or disasters
    - Will be recovered to an operational state within a reasonably short period
Examples of Incidents Requiring Planning

- Loss of information confidentiality
- Integrity compromise
- Theft or damage of physical IT assets
- Denial of service attack
- Misuse of services, information, or assets
- System malware Infection
- Attempts at unauthorized access
- Unauthorized changes to organizational hardware, software, or configuration
- Reports of unusual system behavior
- Responses to intrusion detection alarms
- Loss of one or more critical servers
- Internal network disruption
- External IT network disruption server
- Telecommunications disruption
- Loss of website or other external facing application
- Loss of access to an Internet service or SaaS, such as Salesforce, Dropbox, etc.
- Unavailability of a work facility
- Unavailability of key personnel
How IR/BCP Fits into the Information Security Management Chain

Identify | Protect | Detect | Respond | Recover

Incident Response Planning
Business Continuity Planning

How well can you detect, respond and recover?
Incident Response and Business Continuity Objectives

1. Verify that an incident occurred or document that one has not
2. Maintain or restore business continuity while reducing the incident impact
3. Identify the causes of the incident
4. Minimize the impact of future incidents
5. Improve security and the incident response planning function
6. Prosecute illegal activity
7. Keep management, staff and appropriate clients informed of the situation and response
8. Apply lessons learned to improve the process
Planning Requires Information Gathering and Analysis

- Names, roles and contact information for the Incident Response Team (IRT), staff, vendors and key clients
- Regulatory, contractual and compliance requirements
- Business Impact Analysis
- Recovery procedures for various scenarios
- An inventory of all technology: hardware, software, SaaS
- An inventory of all needed connectivity
- An inventory of critical IT documents
- Location of all critical business information, including back-ups and shared folders
- Location of passwords and encryption keys
- An inventory of vital business records
The Incident Response Team (IRT)

- Responsible for working with Information Security Manager to manage recovery from an information security incident or disruption in accordance with the plan.
- Chair: Information Security Manager (ISM)
- Member(s) of executive team
- CIO, IT Director &/or IT Vendor
- Information security subject-matter experts
- In-house or external counsel
The 5 Phases of Incident Response and Business Continuity


Incident Response Management

References:

© Copyright 2015. Citadel Information Group. All Rights Reserved
Business Impact Analysis: What order do you restore? What is needed to restore?

- List of business functions
- Description of the operational and financial impact of disruption
- The level of impact of a disruption of the function
- Maximum tolerable downtime (MTD)
  - Total time the system owner is willing to accept for a mission/business process outage or disruption
- Recovery time objective (RTO)
  - Maximum amount of time a resource can remain unavailable before there is an unacceptable impact
- Recovery point objective (RPO)
  - Point in time prior to an incident to which business process data must be recovered
- External functions this function depends upon
- External functions dependent on this function
- IT resources needed to maintain business function (hardware, software, telecommunications, etc.)
- Staff resources needed to maintain business function
- Any special security considerations, including confidentiality
A Plan on the Shelf Isn’t Worth the Paper Its Printed On

- Provide training to staff at least annually and when major updates are developed
- Conduct “table-top” simulations at least semi-annually
  - Incident Response Team, outside vendors, CFO, attorney(s) and others semi-annually
- Test backup/recovery and other high risk procedures at least quarterly
- Update plan as people and circumstances require
- Review plan at least semi-annually and update as necessary
Lessons Learned: Doing It Better Next Time

- How did event happen?
  - Root cause analysis

- What was the damage (direct and indirect costs) and cost of containment?

- What user training might have prevented the incident?

- What changes in policies or procedures might have prevented the incident?

- What additional equipment or technologies might have prevented the incident?

- How was response handled? How could it be improved?

- Was initial response timely?

- Was containment and restoration timely?

- Was right documentation available?

- If law enforcement was involved, did it help or hinder the response?
  - How could relationship with law enforcement be improved?

- Were appropriate parties informed in a timely manner?

- Were response procedures sufficient?

- How do we get “lessons learned” into “corporate DNA?”
Information Peace of Mind®

Information Security Proactively Managed
Commerncially Reasonable Information Security Practices
Lower Total Cost of Information Security™
Citadel Information Group: Who We Are

Stan Stahl, Ph.D
Co-Founder & President
35+ Years Experience
Reagan White House
Nuclear Missile Control

Kimberly Pease, CISSP
Co-Founder & VP
Former CIO
15+ Years Information Security Experience

David Lam, CISSP, CPP
VP Technology Management Services
LABJ CIO of Year
20+ Years Information Security Experience
Citadel Information Group: What We Do

Deliver *Information Peace of Mind*\(^{\text{SM}}\)

to Business and the Not-for-Profit Community

**Cyber Security Management Services**

Information Security Leadership

Information Security Management Consulting & Coaching

Assessments & Reviews ... Executive Management ... Technical Management

Secure Network Engineering ... Secure Software Engineering

Incident Response / Business Continuity Planning

Adverse Termination
For More Information

Stan Stahl  Stan@citadel-information.com  323-428-0441
LinkedIn: Stan Stahl  Twitter: @StanStahl

Citadel Information Group:  www.citadel-information.com
Information Security Resource Library

Free: Cyber Security News of the Week
Free: Weekend Vulnerability and Patch Report
Be Prepared: Incident Response and Business Continuity Planning

Thank You!

Secure the Village
Cybersecurity Roundtable
June 2016

Stan Stahl, Ph.D.
President
Citadel Information Group

© Copyright 2016. Citadel Information Group. All Rights Reserved.