Crafting A Plan for When Security Fails

OWASP
The Open Web Application Security Project
Robert Lelewski
IBM’s Emergency Response Service
Senior Incident Response Analyst and CSIRP Development Lead
Immersed in the forensics and incident response world since 2004

The Usual Security Certs:
CISSP, CISA, CISM, EnCE, CCE, etc.

Former Ski Train conductor!
Agenda

• What is a CSIRP and why have one?
• Examples of Fail and Success
• CSIRP Success Factors
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
• What is a CSIRP and why have one?
• Examples of Fail and Success
• CSIRP Success Factors
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
**Computer Security Incident Response Plan**

CSIRPs come in many different names but have the same goal:

Apply a pre-approved process and methodology to address computer security incidents in order to allow an efficient and coordinated response.
My experience with CSIRPs...

Incident Response Experience:
• Involved in hundreds of client emergencies, large and small
• Able to view what has and has not worked during incident response
• Develop custom CSIRPs for large, international companies in various sectors
Show of Hands!

How many in the audience work for a company that has:

- A CSIRP?
- Updated their CSIRP in the last 9 months?
- Conducted a mock incident in the last 9 months?
- A specific person assigned to maintain your CSIRP?
- Pre-printed copies of your CSIRP?
- A plan consisting of someone yelling ‘PANIC!’ and 40 people jump on a conference line?
  - The Costanza Option
Why is a CSIRP Important?

1. Saves time
2. Defensible, pre-approved methodology
3. Ensures the appropriate notifications
4. Communications structure
5. Easier to gather appropriate resources
6. Quicker resumption of operations
• What is a CSIRP and why have one?
• **Examples of Fail and Success**
• CSIRP Success Factors
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
Scenario:
A large bank experienced a successful SQL injection attack. Initial indicators demonstrated a high likelihood customer data was compromised.

The People:
Skilled, qualified to be in their positions, and seemingly excellent people to respond to the incident.
What went wrong?

1) Took four hours to find where the CSIRP was located.
2) Practice? What practice?
3) No clear person in charge or an apparent chain of command.
4) Executives jumping into the trenches.
5) No one notified regulatory agencies.
6) Blame was assigned.
7) CSIRP was not flexible to accommodate the situation.
Example of Fail

End result?

An incident that would have normally taken only a few days to address became a long, drawn out affair. Simply put, it was a mess.
Scenario:
A medium sized, publicly traded chemical company had information posted on PasteBin about the ability to access restricted URLs with customer information.

The People:
Skilled, qualified to be in their positions, and seemingly excellent people to respond to the incident.
Example of Success

What went right?

1. Key decision makers were quickly. Required attendees only.
2. Clear authority.
3. Redundancy.
4. Regulatory team was brought into the response early.
5. Statements to media and investors came from one source.
6. Key system owners with proper credentials were able to be immediately contacted.
7. Proper after action review occurred.
End result?

The incident was treated with the proper level of severity. Regulatory considerations were brought forth early on in the engagement. Coordinated, preplanned response.
Breaking down the issues with the bank and the chemical company...

1. Internal communication
2. Regulatory Issues
3. Blame
4. Flexible CSIRP
5. Who’s in charge?
6. Not including the proper people
7. Cyclical process
• What is a CSIRP and why have one?
• Examples of Fail and Success
• **CSIRP Success Factors**
  – **Internal Communication**
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
The number one issue we see during incidents is not properly managing internal communication.
What went wrong?
1. Who is in charge?
2. Is this a coordinate response?
3. Siloed information and response?
4. Individual effort or a team effort?
How does this help?
1. Clear, preapproved lines of communication
2. Key decisions makers are informed of all information
3. Executive management is kept in the loop
4. Organized, efficient response
• Technical
• Must understand incident response and security
• Comprehends threat landscape
• Calm under pressure
• Knowledge of technical layout of the organization
• Moderately technical
• Able to present well
• Understand business goals and risks
• Have an intimate organizational knowledge
• Respected by C-Level executives
• Invested in the CSIRP process
A clear chain of command also reinforces who is in charge.

- No diffusion of responsibility
- Accountability
- Investment in the CSIRP process
• What is a CSIRP and why have one?
• Examples of Fail and Success
• CSIRP Success Factors
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
We live and work in a highly regulated environment.

- PCI
- HIPAA
- SOX
- Individual state disclosure rules (California)
- Etc.

Depending on the regulation, disclosures may need to be reported within five days of a suspected release.
How do we remedy this?

Create tripwires to include relevant regulatory experts.

As soon as it is possible information may have been accessed by an unauthorized party, the regulatory committee gets pulled in.
Regulatory Issues

Strategic Team

Incident Officer

Incident Manager

Regulatory Committee
The regulatory committee is notified by the strategic team as soon as they may need to be involved.

- ‘Plugged in’ as needed and not a part of every incident.
- Briefed, may ask clarifying questions, convey their concerns, etc.
- They do not jump into the trenches.
A committee approach may be applied towards other sensitive issues (e.g., brand management, corporate security).

Creates buy in from the committee members
Spreads knowledge of the CSIRP process
• What is a CSIRP and why have one?
• Examples of Fail and Success
• **CSIRP Success Factors**
  – Internal Communication
  – Regulatory Issues & Committees
  – **Blame**
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
“Mary’s weak password caused this event.”

“Joe failed to secure the application.”
It is not the role of the core incident response team to assign blame. Why?

- Knowledge is rapidly changing.
- Statements may hurt reputation.

Ensure this is reinforced in trainings and mock incidents.
Blame

Incident Officer

Strategic Team

Incident Manager

Human Resources
Agenda

• What is a CSIRP and why have one?
• Examples of Fail and Success
• **CSIRP Success Factors**
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – **Cyclical Nature**
  – Tiered and Flexible CSIRP
  – Resources
• Recap
• Treat the CSIRP like a living document
• Not to be dusted off only during emergencies
• Preparation and after action often neglected
Cyclical

OWASP
The Open Web Application Security Project

Preparation → Detection & Analysis → Containment Eradication & Recovery → Post-Incident Activity

Source: NIST
• What is a CSIRP and why have one?
• Examples of Fail and Success
• **CSIRP Success Factors**
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – **Tiered and Flexible CSIRP**
  – Resources
• Recap
Incidents need to be classified with at least three tiers of importance.

- Avoids panic at every incident
- No ‘crying wolf’
- Ensures truly bad incidents are treated as such
Does your CSIRP address:
• Threat Based
  – Limited value
  – Process breaks down for undefined threats

• Symptom Based
  – Plan for emerging threats
  – Covers USB eating locusts
Examples of Symptom Based Standards:

– Minimal risk of the unresolved problem getting worse or spreading to other areas of the organization.
– Potential risk...
– Medium to high risk...
– High risk...
Examples of Symptom Based Standards:

• Limited to very few individuals and/or systems.
• Limited to single department and/or non-critical application
• Event affects several locations and/or systems and/or applications with a direct business impact.
• Event affects worldwide operations and/or systems and applications critical to the business
• What is a CSIRP and why have one?
• Examples of Fail and Success
• **CSIRP Success Factors**
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – **Resources**
• Recap
- People
- Money and Contractors
• Must be able to pull employees from normal jobs
  – Authority
  – CSIRP emergencies take priorities
Money and Contractors

Incident Manager must be able to quickly allocated equipment and necessary contractors

- Small slush fund (~$2,500)
- Pre-approval to include certain contractors
• What is a CSIRP and why have one?
• Examples of Fail and Success
• CSIRP Success Factors
  – Internal Communication
  – Regulatory Issues & Committees
  – Blame
  – Cyclical Nature
  – Tiered and Flexible CSIRP
  – Resources
• Recap
Wrapping It Up

• Control communication
• Symptom vs. threat based
• Committees can be your friends
• Cyclical process
• No blame
• Resources
Thank you!

Robert Lelewski
RLELEWSKI@US.IBM.COM
720.271.5130