



Incident Management

Mitigation and Remediation

Presented By Carl Grayson

- The Why
- The What
- A (very) little bit of How
- The Who
- Preparation going a long way
- Some “probably good to do this” and some “don’t try this at home”

- THE ISSUE

- Almost all “good practice” standards specify Incident Response planning now (Sarbanes-Oxley, ISO, IEEE, ITIL, Payment Card Industry, etc)
- Unfortunately, security probably will fail in your organisation at some point; how bad it will fail is the real question
- It’s a lot like DR/BCP – requires (re-)planning, education and testing in a perpetual cycle
 - Will likely be put into action more frequently than either

- ADVICE

- Prepare beforehand for an Incident
 - Developing a Response as an Incident is occurring probably will create more stress, cost more, take more time and not be as well executed

- THE ISSUE
 - Different types of Incidents have different impacts for different organisations
- ADVICE
 - Map types of Incidents and how you Respond against your business model
 - Generally speaking, goals usually fall along the lines of
 - Return to business as usual as quickly as possible
 - Determine and eliminate root cause(s) of the failure
 - Recover losses where possible
 - (Keep additional costs and disruption to a minimum)
 - Make sure you keep **your** goals in mind
 - Some incident categories may be of little or no importance to you
 - Others may ruin you – pick the media-hyped incident of your choice

- Identification and Categorisation
 - Finding out what's going on and deciding whether it's something to investigate
 - Getting a first look at the nature of the problem
- Containment
 - Deploying the Incident Response Team, evidence acquisition and assessment of options for limiting impact
- Eradication
 - Root cause and threat determination → elimination
- Recovery
 - Getting back into operation and recovery of losses if possible
- Follow-up
 - How well did this Incident get dealt with?
 - Probably the most neglected part of Incident Management

- The more rigorous you want to be, the more paperwork you'll need
 - Legal options may require forensically sound evidence with chains of custody and descriptions of all activities undertaken throughout the incident
- Activity trails will help with later reviews of the Incident
- Is there enough "oomph" in your Policies to allow investigation?
- Do you have clauses for investigations in your contracts?
 - Employees?
 - Third Parties?
- Do you have procedures in place so people know what to do?
- Do you have template forms, reports and checklists ready so you don't forget things during and after an Incident?
 - For example, Chain of Custody forms for evidence; management update reports; actions when acquiring evidence?

- THE ISSUE

- Incidents usually require a time-sensitive response – if staff don't know what to do, critical information and options may be lost

- THOUGHTS

- Do general staff know who to contact?
- Do each the Incident Response Team members know what might be expected of them?
- Don't underestimate the value of practice runs
 - Provide familiarity with process – greater speed and correctness
 - Exposes weaknesses in procedures very quickly

- THE ISSUE
 - Under stress it is good to know who is capable and permitted to decide time-critical issues
- CONSIDERATIONS
 - Who will run the Incident Handling Team?
 - Somebody trustworthy with technical and commercial awareness
 - Which team member has authority to make (potentially costly) business decisions?
 - A business representative or delegate who can also keep upper level management informed
 - Who can translate what is going on between the technical and non-technical team members?
 - Probably not best to assign this to one of the team working directly on the response – they'll be too busy

- Team is pan-organisational and not just technical
 - We need to run a business here!

- *Everybody* has an opinion (trust me)
 - Some valid
 - Security, Risk, Operations, Business, Public Relations, Legal, Human Resources...
 - Some not so much
 - Operations, general staff, the receptionist, the janitor...

- Hopefully, this one is obvious...
- Somebody who knows how to run an Incident intimately:
 - Rules of engagement
 - Who to talk to
 - How to get things done

Somebody who can determine if it really is a security problem

- Somebody who understands Risk Management
 - Because sometimes it isn't worth chasing
- Security people can be a bit too paranoid
 - Mind you, they are also often right

- Subject Matter Experts on whatever technologies you use
 - These people usually really do know their systems – use them!
- Be a little careful; these are sometimes the perpetrators
- Can be a little precious about their systems
 - Some forensic practices can go against the primary goals of Operations (keep things running at all costs)
 - Can be defensive if they know they haven't exactly followed the book
 - Take care to differentiate from malice

- Varied and can depend on the type of Incident and structure of the Organisation
- May include:
 - System Owners
 - Information Owners and Custodians
 - Function Owners
- Somebody with Financial Authority!
 - Can be an expensive exercise
 - Costs can move rapidly
- This crowd is generally risk tolerant
 - Can be hard to get them to accept outages

- TJX just lost 45.7 million credit cards
 - Is there a positive spin?

- Information tends to leak... eventually
 - Employees gossip
 - Disclosure laws

- May be able to help with internal stories

- These people find silver linings in almost everything
 - Can be good for morale at 2:30 a.m. if nothing else!

- The Organisation's authority on
 - Laws
 - Regulations
 - Contracts

- Are usually fairly conservative

- Generally don't bite (much)

- Obvious if the issue is internal malicious staff
 - Sometimes need to tread carefully → go directly to Legal, don't pass Go...

- Are often the internal communications channel
 - Cover stories necessary?
 - Policy reinforcement and interpretation

- Less often considered for monitoring of Response staff workloads and stress
 - Could be long hours
 - Overtime?!?
 - Personal commitments

- Consider having an Incident Operations Hub (the "War Room") with specific outgoing channels and messages
- Who are the authoritative sources for each type of information?
- Externally focused communications
 - Police (for discovered criminal acts)
 - Media (what's the spin?)
 - Customers (you may be legally or contractually obligated to)
 - Partner organisations
 - Investigative pursuit
 - Due diligence
- Internally focused communications
 - Staff – there is *always* a rumour mill
 - Personnel privacy considerations for internal malice

- Resource constraints
 - Incidents can take place at any time
 - They can divert a significant number of personnel from their normal routines
 - Company functions can be disrupted by both the Incident itself *and* the Response (e.g. risk mitigation, evidence acquisition)
 - Staff generally don't work too well after the first 16 hours or so
- Operational contention
 - Business operational staff are generally focused on keeping things running at all costs – what are your priorities (go back to Point 1)?
- Detailed Incident Response procedures aren't linear
 - Use common sense at all times to continually evaluate options

- Ignoring the Incident once things are working again
 - We've seen companies go back into operation while still compromised and without removing vulnerabilities
 - Good revenue for us – we get to come back and find the same compromise!
 - Learn from mistakes and try not to make it a blame game
- Panicking and overreacting
 - I've seen companies report odd events to the Police, only to find out that it was actually normal business functioning
- Giving out imprecise or unclear information
 - The worst interpretation is always the one people believe

<http://www.security-assessment.com>
carl.grayson@security-assessment.com