Getting the CIO and CISO talking the same language

INCIDENT RESPONSE

DAVID SHEIDLOWER, CISSP, CISM

Today's discussion: incidents

ID	what are they	ID.RA-4
PR	how do we make sure they don't happen	PR.IP-9
DE	how do we know when one has happened	Most
RS	how do we respond	Most
RC	how do we recover	Most

- A CISO's definition of an incident is not the same as the ITIL definition. The latter is the definition that aligns with the CIO's Service Delivery model. Security may classify incidents in terms of risk or potential harm whereas IT may classify them based on SLA's. In this session we will walk through the steps for security incident response and discuss the features of a robust incident response program including documentation, the formation of the incident response team and root cause analysis.

What is an incident?

- **Security:** an occurrence that **actually or potentially** jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies
- **ITIL 2011:** an unplanned **interruption to an IT Service** or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident — for example, failure of one disk from a mirror set.

Why “potential” matters

- If you wait to identify events as incidents till you are sure how they actually impact your organization, you might be too late and/or your response might be slow
- Events that point to potential impacts/likelihoods can be an indicator of a vulnerability or compromise (the canary is still breathing but it’s coughing an awful lot)
  - In the language of safety: A Near Miss is an unplanned event that did not result in injury, illness, or damage – but had the potential to do so. Only a fortunate break in the chain of events prevented an injury, fatality or damage; in other words, a miss that was nonetheless very near. (National Safety Council)
- In other words, Security cannot always wait for there to be an “unplanned interruption”

How do we prevent them?

- An incident occurs when preventive controls are insufficient in that one specific case and that weakness is exploited

But that does not mean we accept incidents; we respond

- You make sure your controls are strong and effective to prevent incidents. But once they happen, you respond
- Response begins with pre-planning. But once an incident occurs, response begins with detection

What risk does an incident pose?

What risk does an incident pose?

- Organizational Risk is a function of impact and likelihood in the presence of mitigating controls
- The likelihood of an incident that has already occurred is 100%
- The only risk-based response therefore needs to control for impact
- Being prepared to respond to an incident is crucial in controlling for impact

Why types matter

- Incident response requires an initial assignment of severity, i.e. impact
- The more comprehensive your list of incident types and their corresponding severity, the faster you can respond appropriately
- Examples of types:
  - Denial of Service
  - Breach of Confidential data
  - Lost/Stolen device(s)
  - Ransomware/Malware outbreak

Detect: I know an incident when I see one

True story

- A hospital installed a new operating room scheduling system that also tracked surgical complications. One surgeon had a significantly lower complication rate than his peers. A review of the detailed records revealed he was not recording a number of events as complications and if he had, his rate was average. When asked why he was not recording those events he replied “those aren’t complications, those things just happen sometimes.”
- Lesson learned: incidents need not be unusual

Not believed to be a true story

- An organization implemented a detective control. The control sent a number of alerts that turned out to be false positives and as a result the organization began to de-prioritize their response to the alerts. So, when the control was actually reporting an exploit…

…the wolf ate all the sheep and
ate the detective control as well.

- Lesson learned: don't ignore or fully tune out false positives

Everybody's business to detect

- Detecting an anomalous event is the responsibility of virtually everyone in the organization
- For incident response to be effective, reporting an incident should be as standard and easy as possible
  - No wrong door
  - No passing the buck on initial record/ticket
- From there, the initial response needs to zoom in and triage

Zooming in

- A date and time stamped ticket should be opened as soon as an incident is detected/reported
- Level 1 support must be trained to triage these tickets
  - Ones they can resolve (encrypted laptop left at airport security)
  - Ones they should not (an office manager reporting ransomware on 10 machines)
- Alerts from automated systems should be triaged by workflow and often pass over level 1 altogether
- After initial triage: zoom out

Zooming out

- Procedures should be in place already to determine who is on point for managing the initial response to the incident
- That individual, often from Security or IT
  - needs to be well trained in incident response
  - assigns initial severity if has not been done yet
  - begins to document dates, times, evidence of compromise, parties involved, data involved and initial actions taken
  - at the same time, determines if there needs to be a broader focus: an incident response team
    - determination should be based on established criteria

The IRT

- The Incident Response Team is formed when there is potential for an incident to cause significant impact to the organization
- It is the team of “responders” and should be made up of appropriate stakeholders from within the organization
- Can include (but not limited to)
  - Legal
  - Finance
  - OPS
  - IT
  - Communications
  - Compliance
  - HR
  - Security[2]

The IRT's agenda

- What happened
- What was the impact/actual severity
- Who needs to do what
- Who needs to be told what
- Do we need help
- Are we the right people to resolve this

Got clients?

- If you have clients and if the incident involves data about them or team members that work on their accounts then the IRT MUST determine if client notification is called for and if so should involve the executives over that client account
  - This is more than just a contractual issue
- If Personally Identifiable Information (PII) is involved, involve counsel ASAP

Housekeeping

- Someone on the IRT is responsible for recording decisions and actions
- Someone (perhaps the same person but not always) ensures that evidence is collected and stored securely
  - If chain of custody is a potential concern, involve counsel ASAP
- For larger incidents, these should be very formal roles

Closing v. Resolving

- An incident is resolved when normal service is restored and/or serice is otherwise restored to the impacted users (referred to as *incident management* in ITIL)
- An incident is closed when root cause analysis is complete and all investigations are concluded
- An incident can be closed even though there are additional action items that come out of it
  - Retiring servers/patching
  - Additional staff training
  - Communicating with consumers
  - Risk assessment

Train, Test, Drill

- Train people who are likely to respond to an incident in the policies, tools and procedures for response
- Test your procedures
  - Don't tell people when an external pen test, phishing test or other vulnerability probe is happening. Measure responses to these "safe" attacks
- Run drills to walk through the procedures and discuss scenarios. Drills can surface "what ifs" and let's you adjust your procedures accordingly.

Thank you.