Building Capability and Community Through Cyber Incident Response Exercises

Matthew Ricks
Stanford University

Ivy+ Cybersecurity & Privacy Festival 2021
The Future of Work
Agenda

- Practical steps with examples for planning and conducting recurring exercises

- Sharing experiences

- Call to action
Recurring Incident Response (IR) Exercise Cycle
Prerequisites for holding an Incident Response (IR) Exercise

- You have an existing IR plan (preferable)
- OR: You are in the process of developing an IR plan
- You have initial leadership support (with intent of ongoing support)
- You have existing tools and processes to detect and report an incident

Leverage NIST SP800-61 Computer Security Incident Handling Guide
Must address elements of preparation, detection, analysis, containment, eradication, recovery
Recurring Incident Response (IR) Exercise Cycle

- PLAN
- CONDUCT
- ASSESS
Debrief prior exercise, chart course for next exercise

- This is the first step of the PLAN phase and last step of the ASSESS phase
- Review feedback from prior exercise (plus/delta, survey results, etc.)
- Review objectives, discuss any changes or additions
- Get leadership direction on desired area of focus and type of exercise (mix it up, keep it fresh)
- Propose which groups to involve in the exercise
- Agree to timeframe for exercise
- Leadership assignment of Subject Matter Experts (SME’s) to participate in planning and facilitation
Brainstorming

- Hold kick-off meeting with assigned SME’s
- Leverage a collaboration platform (like Google) to create and store exercise documents
- Review feedback from leadership
- Review feedback from prior exercise
- Consider current and upcoming events (local, regional, world), latest risk assessment, current threats, recent incidents, and regulatory changes -- all which may serve as the backdrop and provide context
- Discuss any changes within the organization or infrastructure
- Brainstorm possible scenarios
- Identify specific groups to participate, based upon scenarios
- Gather info and intelligence on areas and groups which may be in scope
Narrowing

- Confirm specific details and which individuals to invite
- Develop agenda
- Finalize objectives, exercise artificialities
- Finalize scenario(s), based upon confirmed participants
- Develop and fine-tune Master Scenario Events List (MSEL)
- Produce detailed injects
- Complete slide deck for exercise
- Finalize logistics
Logistics

- Day of week – Monday vs. Friday
- Time of day – morning vs. afternoon vs. through lunch
- Duration, including breaks
- Location – daily operational area vs. special conference room
- Invitations and reminders
- Room configuration – round vs. rectangular tables, comfort of chairs, power strips, wi-fi
- Food – hot and cold caffeine, sugar
- AV – display, mic & speakers, video conferencing (if necessary for remote participants)
- Table name tents, name badges (if necessary)
Day of the Exercise:

- Welcome
- Introductions
- Leadership message
- Primer/Refresher (topical)
- Review objectives and instructions (artificialities)
- Context
- Exercise
- Checkpoint
- Report-out
- Gather feedback
- Next steps
## Example Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00am - 10:30am</td>
<td>Welcome, Introductions, Message from Michael, HIPAA Refresher, Objectives, Instructions, Context</td>
</tr>
<tr>
<td>10:30am</td>
<td>Begin exercise</td>
</tr>
<tr>
<td>11:15am</td>
<td>Checkpoint</td>
</tr>
<tr>
<td>11:30am</td>
<td>Grab lunch</td>
</tr>
<tr>
<td>12:30pm</td>
<td>Conclude exercise</td>
</tr>
<tr>
<td>12:30pm - 1:00pm</td>
<td>Complete incident investigation reports</td>
</tr>
<tr>
<td>1:00pm - 1:45pm</td>
<td>Incident Investigation Report Reviews, Group +/Δ (individual feedback via Qualtrics survey)</td>
</tr>
<tr>
<td>1:45pm - 2:00pm</td>
<td>Next steps</td>
</tr>
</tbody>
</table>
Example Exercise Objectives

- Exercise our incident response plans; make note of necessary improvements.
- Leverage and validate communication channels.
- Complete Incident Investigation Report for each incident.
- Gain familiarity working with key participants in response to incidents.
- Have some fun together!
Example Exercise Artificialities

- Information may come in via various formats, including email, Slack, shares from Google, ServiceNow, phone calls, and walk-ups.
- Options for providing updates or asking questions: Send email to simteam@lists.stanford.edu; include “EXERCISE:” in the subject line or Walk up to the Simulation Team table.
- Simulation Team will periodically wear different hats to denote different roles that are communicating or being communicated to.
- Liberties have been taken with certain technical realities and timeframes for the purpose of exercising our incident response plans.
- For written communications required, capture the idea; you don’t need to wordsmith or worry about quality or approvals.
- Tables simulate the physical barriers/buildings; if you need to collaborate, walk over to another table. If there is somebody not in the room that you need information from, go ahead and call them or message them.
## Example Scenarios

<table>
<thead>
<tr>
<th>Lost/Stolen Laptop</th>
<th>Server infected by ransomware</th>
<th>DDoS Attack</th>
<th>Spear phishing campaign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website compromise or defacement</td>
<td>DNS compromise</td>
<td>Breach that triggers HIPAA notification</td>
<td>SCADA system compromise</td>
</tr>
<tr>
<td>Digital signage system compromise</td>
<td>Insider abuse of privileges</td>
<td>Data breach and exfiltration</td>
<td>Database breach through malware</td>
</tr>
<tr>
<td>Data exposed in a public cloud service</td>
<td>User requests “right to be forgotten” per GDPR</td>
<td>Server compromised and used for crypto-mining</td>
<td>Transaction application compromise</td>
</tr>
</tbody>
</table>
# Example Master Scenario Events List (MSEL)

<table>
<thead>
<tr>
<th>Inject #</th>
<th>Delivery Time</th>
<th>Actual Time</th>
<th>To</th>
<th>From</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A</td>
<td>12:45</td>
<td></td>
<td>Privacy Office</td>
<td>Jurgen K</td>
<td>Phone Call (recorded, message left on the Privacy Office line):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Hi Privacy Office - My name is Jurgen. I'm the PI for a research project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>examining the role of Stanford in the ongoing, worsening global</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>displacement crisis and I have an incident to report - can someone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>call me back as soon as possible? My number is 650-555-9634.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Expected Action:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Privacy Office calls back and asks for more information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• May ask to fill out a lost/stolen device form</td>
</tr>
<tr>
<td>5A</td>
<td>1:50</td>
<td></td>
<td>ISO</td>
<td>Maria G</td>
<td>Alert (Email sent by Google Security Command Center to Maria G)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SimTeam to share to John T and Sarah V:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://drive.google.com/open?id=1oBBbyVEPe8k-rZq3QM84_cXtJRsByQDj">https://drive.google.com/open?id=1oBBbyVEPe8k-rZq3QM84_cXtJRsByQDj</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...there was unusual activity on one of the machines they manage...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Expected Action:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• ISO should inquire as to who is the business owner and what data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>resides on this machine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• ISO should reach out to Jurgen K to ask questions</td>
</tr>
<tr>
<td>7</td>
<td>2:15</td>
<td></td>
<td>Everyone</td>
<td>CNN</td>
<td>Display in main slide deck the mocked-up story about kidnapping of</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>researcher</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Displayed in main slide deck for exercise</td>
</tr>
<tr>
<td>8</td>
<td>2:20</td>
<td></td>
<td>Michael D</td>
<td>Jane S</td>
<td>In-person request from Jane to Michael for an update to take into a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Board meeting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Hi, Michael. I am going into a Board meeting at 3pm and I’d like to take</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>an update on the incident into the meeting just in case I am asked about</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>it, so would you please debrief me at 2:50?”</td>
</tr>
</tbody>
</table>
Example Injects
Example Injects

From: "Daktronics Support" <support@daktronics.com>
Date: Thursday, March 09, 2017 11:32 PM
To: DAKTIS Support <support@stanford.edu>
Subject: DakaTIS ALERT: Signage under active attack

Earlier today, we announced a critical vulnerability in the remote administration feature of our Premier line of digital signage. As before, we advise you to patch your administrative systems as soon as possible.

We have also recently learned that this vulnerability is being actively exploited by a political organization that calls it "Don't Trust on Air!" The source for these attacks have been traced to systems based within a single datacenter in France.

If for some reason, you are unable to patch your administrative systems, we have been informed from our customers that the following IP addresses should be blocked at perimeter:

144.213.192.0/22
144.217.128.0/18
144.217.61.24
144.217.32.128
144.217.32.64
144.217.128.0/18
144.217.256.0/18
144.217.26.0/24

We will update you as we learn of additional source IP addresses.

Sincerely,
Issue Source

Stanford MyDevices

Registered Devices of this inventory

Comment: "My Devices" services

Model: "My Devices" services
Name: "My Devices" services
Type: "My Devices" services
Description: "My Devices" services

We will update you as we learn of additional source IP addresses.

Sincerely,
Issue Source

Stanford Services

Management

Incident BINC005671 has been Assigned to UIT ISO Consulting by UIT Triage Group.

Short description: Received bad phoning email
Priority: 3 - Moderate
Reported by: Richard Walters
Reported To: Richard Walters
Opened: 2017-01-14 10:49:09 PST
Example Injects
CONDUCT  Option: Leverage existing scenarios and situation manuals
CONDUCT  Option: Hold a “distributed only” exercise

Default mode through the pandemic
CONDUCT  Option: Gamify your exercise, turn it into a competition

Everyone has a role

- Executive Leadership
- Incident Response Lead
- Network Analysis Specialist
- Disk Image Forensics Specialist
- Web Server Admin
- System Log Analysis
- Memory Forensics Specialist
- Email Specialist
- Troubleshooting Problems
- Internet
- Domain Expertise
- Server Admin Expertise
- Application Log Analysis
- Malware Analysis
- Phishing Specialist
- Critical Thinking
- Documentation and Scribe
- Communicate
- Work as a team

Game Rules

- Each team will work independently of each other.
- Points can be earned in four ways:
  - Responses to injects along the way.
    - 10 points each
  - Progress reported at 1:30pm checkpoint.
    - Upto 25 points
  - Completeness of Incident Investigation Report(s) and compliance to IR Plan; responses to mini scenarios
    - Upto 100 points for each IR; upto 25 points for each mini scenario
  - First team to correctly respond to bonus questions posted to Slack.
    - 5 points each
- Winning team will be announced at the conclusion of the exercise.

Participants

- Team Member #1 (M&A)
  - Team Member #2 (ET Compliance Services)
  - Team Member #3 (ETIT Compliance Services)
  - Team Member #4 (ETIT Compliance Services)
  - Team Member #5 (M&A)
  - Team Member #6 (ISO 27001 Consulting)
  - Team Member #7 (ISO 27001 Consulting)
  - Team Member #8 (ISO 27001 Consulting)
  - Team Member #9 (ISO 27001 Consulting)
  - Team Member #10 (CampusGuard)

- Team Member #1 (M&A)
  - Team Member #2 (ET Compliance Services)
  - Team Member #3 (ETIT Compliance Services)
  - Team Member #4 (ETIT Compliance Services)
  - Team Member #5 (ISO 27001 Consulting)
  - Team Member #6 (ISO 27001 Consulting)
  - Team Member #7 (ISO 27001 Consulting)
  - Team Member #8 (ISO 27001 Consulting)
  - Team Member #9 (ISO 27001 Consulting)
  - Team Member #10 (CampusGuard)
CONDUCT  Option: Record your “report-outs” for later review
Methods

● Gather group feedback (plus/delta) within the room
● Gather individual feedback via survey
● Insert feedback into a running retrospective
● Review and analyze feedback and trends
● Apply lessons learned back into the IR process/documentation and into subsequent exercises
● Debrief leadership and start the cycle all over again
Gathering Group Feedback

Quarterly Incident Response Exercise - 8/31/16
Plus/Delta

Plus (what worked well? what could be improved?):
- Well planned
- Everyone at separate tables
- Todd initiating conf call
- Good amount of time
- Good pace
- Forced to use existing communication channels
- Seeing everyone in same room, meeting each other
- Good to understand how different groups think about and talk about things
- Learned a lot from each other
- Exposure to what’s important to each other
- Meeting each other

Delta (what didn’t work well? what could be improved?):
- What other channels other than email?
- Have channels established - jabber (wouldn’t work for OGG)
- If emails, use mailing lists instead of individual email addresses
- Overhear each other between tables, make more far apart or in different rooms
- A little unrealistic, not as much confluence of things as would actually happen
- ISO SecOps underutilized and undirected
- Who is driving the incident?
- Email could cause confusion, leaving some out
- Not always clear roles of each group
- Need to clarify communication channels
- Have a mailing list for incident response established in advance?
- Need to further clarify roles in incident response
- Create standing calls for incident response to get all involved
- Assumptions made, since all info wasn’t in one piece (email threads hard to keep up with), then share with those that need to know; need to address privacy issue; intelligent dashboard like on SVN?
- Come up with top 3 things to establish need for privacy on an incident
- Who is on *need to know* list, does it change each time? (privacy circle changes with each incident; should stay as small as possible)
- Must label the mock news story slides with “Exercise” or “Drill”

What worked well with today’s exercise?

- Great interaction among organizational participants
- Realistic scenarios
- Good day of week / time of day
- Better communication, smaller room
- Great to connect with people
- ISO IR plan is solid – Slack channels and Google docs worked well for coordination
- Questions to the facilitators I thought were excellent
- Report outs
- Nice to work with people may not have had a chance to work with previously
Gathering Individual Feedback

Adapted from “Cyber Breach: Designing an exercise to map a ready strategy,” Regina Phelps

<table>
<thead>
<tr>
<th>Exercise Participant Evaluation Form</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The exercise scenario was realistic.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2. The exercise injects were plausible.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3. The exercise length was appropriate.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>4. The exercise encouraged “hands on” participation.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5. Having everyone in the same room was useful.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6. The facilitation was effective.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>7. The exercise was a good use of time.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>8. The exercise was well organized.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>9. The exercise met my expectations.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>10. We should continue incident response exercises quarterly.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>11. I feel prepared to respond to a cyber incident here.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>12. It would be helpful for others to participate in an exercise like this.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>13. Our team is adequately prepared to respond to a cyber attack.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>14. Our plan for responding to a cyber attack is complete.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>15. The exercise met the stated objectives.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

If you have any other observations or suggestions you would like to share, please note them below or on back of evaluation form:
Individual Feedback Survey: Exercise Preparation and Execution

The exercise scenario was realistic.
The exercise injects were plausible.
The exercise length was appropriate.
The exercise encouraged “hands on” participation.
The facilitation was effective.
The exercise was well organized.

5-point survey rating scale:
5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree
Individual Feedback Survey:
Exercise Expectations and Continuation

The exercise was a good use of time.
We should continue incident response exercises quarterly.
The exercise met my expectation.
The exercise met the stated objectives.
It would be helpful for others to participate in an exercise like this.

5-point survey rating scale:
5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree
Individual Feedback Survey: Incident Readiness

I feel prepared to respond to a cyber incident here. Our team is adequately prepared to respond to a cyber attack. Our plan for responding to a cyber attack is complete.

5-point survey rating scale:
5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree
Formula for an Effective Incident Response (IR) Exercise

Prerequisites

- Existing or work-in-progress incident response plan
- Initial leadership input and ongoing support
- Existing tools and processes to detect and report an incident

Engaged participants

+ Subject Matter Expert (SME) commitment
+ Weaving in current events
+ Organizational and institutional knowledge
+ Creativity
+ Business Continuity process orientation

= An effective IR exercise

Effective IR exercises will contribute to more effective actual incident response
Improving Incident Response Capabilities

**Building Capability**
- Testing and improving the IR plan
- Enhancing collaboration
- Improving communication
- Updating documentation
- Developing muscle memory
- Fostering critical thinking
- Combination of repeating and rotating participants may help to uncover blind spots

**Building Community**
- Developing relationships
- Core groups (ISO, Privacy, Legal, Comms)
- Varying groups (different units)
- Rotating SMEs to help plan/facilitate
- Observers/Partners
- Expanding bench strength
- Solving problems together
- Having fun and laughing together
How it all comes together…
https://youtu.be/_5rbBYhwW1k
What have you done to improve incident response capabilities within your own organizations?
Call to Action

- Schedule and conduct an IR exercise
- Apply lessons learned to your IR process/documentation and IR exercise planning
- Repeat (regularly)

CREDITS: Video and photographs: Stacy Lee; Additional photographs: Matthew Ricks
Building Capability and Community Through Cyber Incident Response Exercises

Matthew Ricks
Stanford University