Building Capability and Community Through Cyber Incident Response Exercises

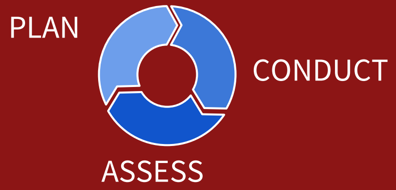
Stanford University

University IT (UIT)

October 2019

Agenda

- Problem Statement
- Why continuity planning professionals should lead cyber incident response exercises
- Practical steps with examples for planning and conducting recurring exercises



- Sharing experiences
- Call to action

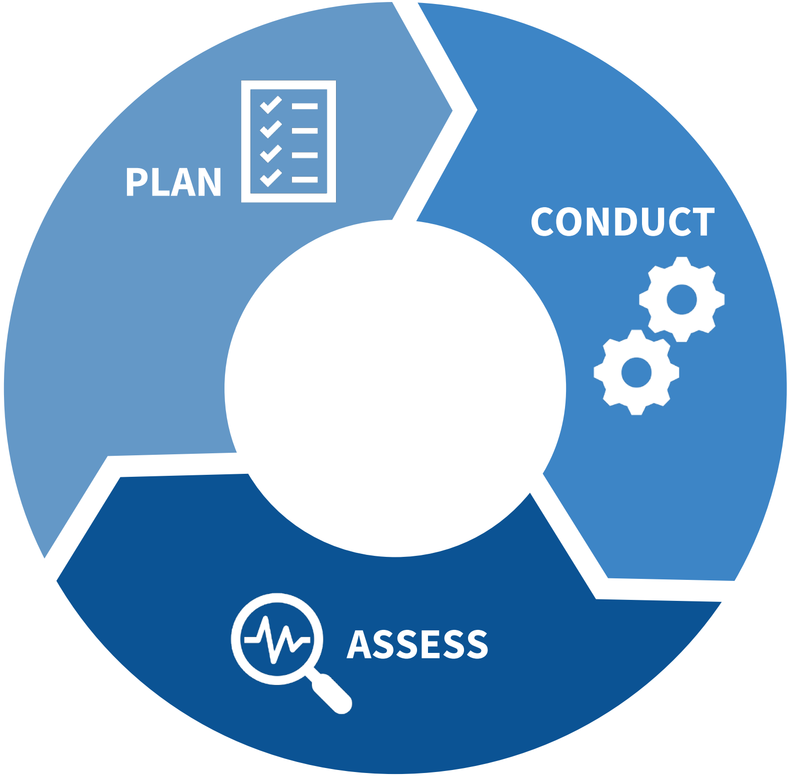
Problem Statement

While a natural disaster or related threat *may* impact your organization at some point, it’s now a given that *all* organizations will eventually experience a cyber attack or breach (if they haven’t been compromised already), making it imperative that you improve your readiness to respond to cyber incidents.

Planning and conducting periodic cyber incident response exercises develops your organization's capability to respond and helps build your community of those who will be better prepared to respond.

Photos of damage on campus caused by the April 18, 1906 “Great Earthquake.” Photos courtesy of the Stanford Archivist

Recurring Incident Response (IR) Exercise Cycle



Why should BCM be inserted into Cybersecurity Incident Response?

Cyber attacks are constantly evolving and occurring more frequently.

BCM has always been a component of Information Security.

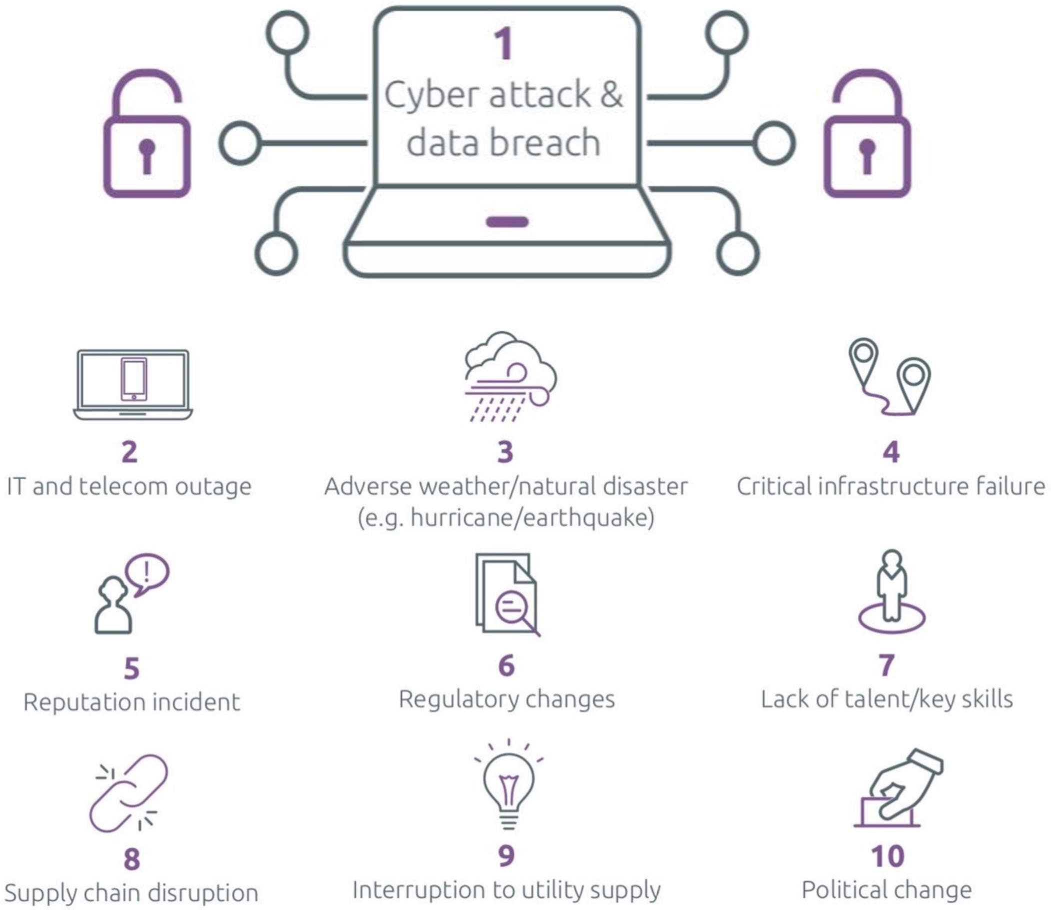
Incidents are identified and contained more quickly when BCM principles are applied.

BCM will be involved in response and recovery, so best to get involved up front.

Build expertise in-house, so you can conduct exercises more frequently without reliance on 3rd party consultants.

Cybersecurity Issues:

#1 Threat



1
Cyber attack & data breach

2
IT and telecom outage

3
Adverse weather/natural disaster (e.g. hurricane/earthquake)

4
Critical infrastructure failure

5
Reputation incident

6
Regulatory changes

7
Lack of talent/key skills

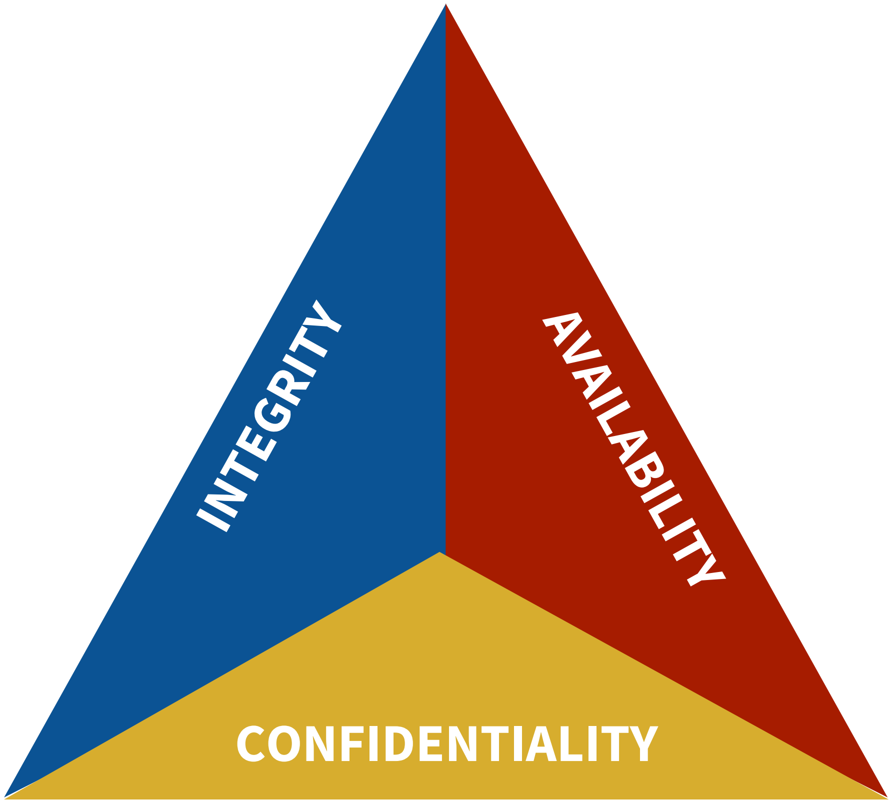
8
Supply chain disruption

9
Interruption to utility supply

10
Political change

Source: BCI Horizon Report 2019

CIA Triad: Goals and objectives of security are equally important to BCM



Intersection of Business Continuity Management and Information Security

DRI Professional Practices 2017

1. Program Initiation and Management
2. Risk Assessment
3. Business Impact Analysis
4. Business Continuity Strategies
5. Incident Response
6. Plan Development and Implementation
7. Awareness and Training Programs
8. Business Continuity Plan Exercise, Assessment, and Maintenance
9. Crisis Communications
10. Coordination with External Agencies

BCI Good Practice Guidelines 2018 – Professional Practices

1. Policy and Program Management
2. Embedding Business Continuity
3. Analysis
4. Design
5. Implementation
6. Validation

(ISC)2 CISSP Domains

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Intersection of Business Continuity Management and Information Security

DRI Professional Practices 2017

1. Program Initiation and Management
2. **Risk Assessment**
3. Business Impact Analysis
4. Business Continuity Strategies
5. **Incident Response**
6. Plan Development and Implementation
7. Awareness and Training Programs
8. **Business Continuity Plan Exercise, Assessment, and Maintenance**
9. **Crisis Communications**
10. **Coordination with External Agencies**

BCI Good Practice Guidelines 2018 – Professional Practices

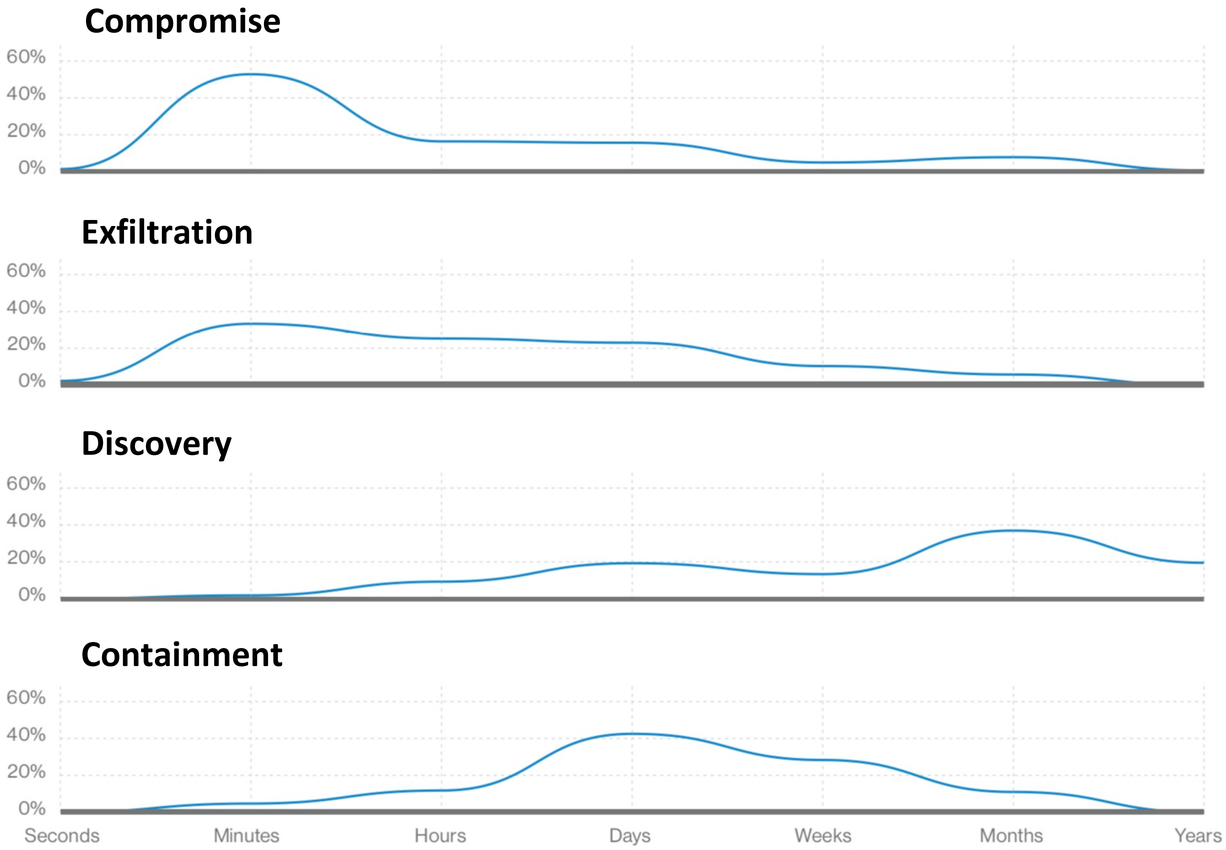
1. Policy and Program Management
2. Embedding Business Continuity
3. **Analysis**
4. Design
5. **Implementation**
6. **Validation**

(ISC)2 CISSP Domains

1. **Security and Risk Management**
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. **Security Assessment and Testing**
7. **Security Operations**
8. Software Development Security

Breach timelines: Time is not on your side

Compromise and Exfiltration can take minutes, Discovery can take months, Response must be more timely



Compromise

Exfiltration

Discovery

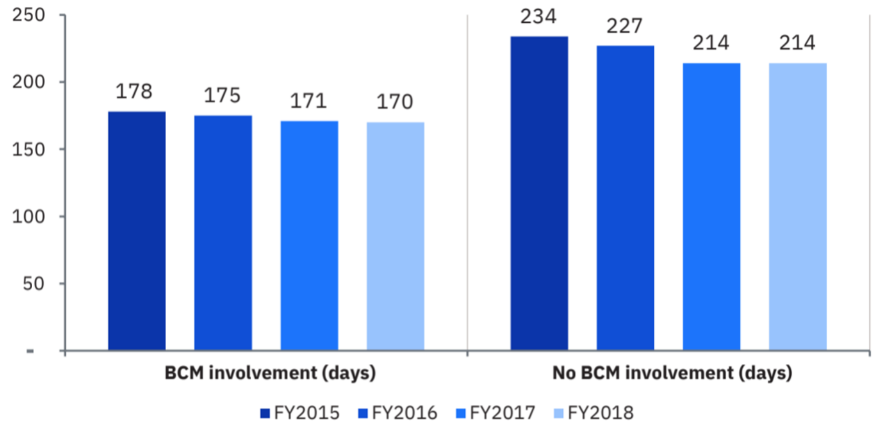
Containment

Source: 2019 Data Breach Investigations Report, Verizon

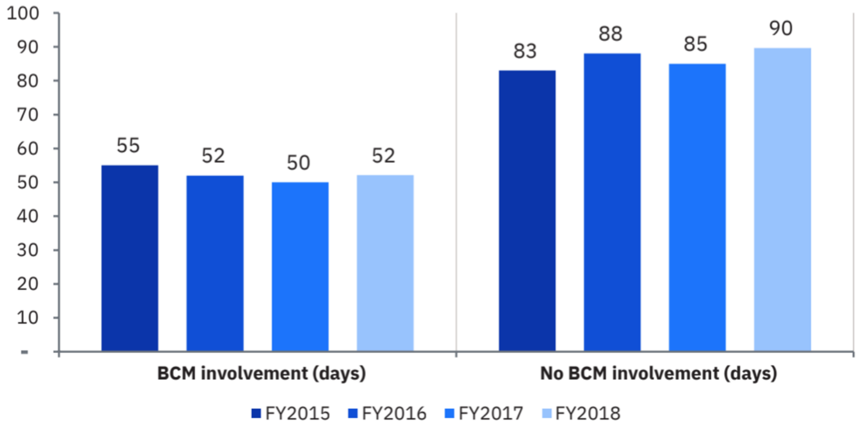
BCM involvement improves Incident Response (TIME)

Mean Time to Identify (MTTI) and Mean Time to Contain (MTTC) for organizations that involve or fail to involve BCM in the IR process

MTTI Comparison



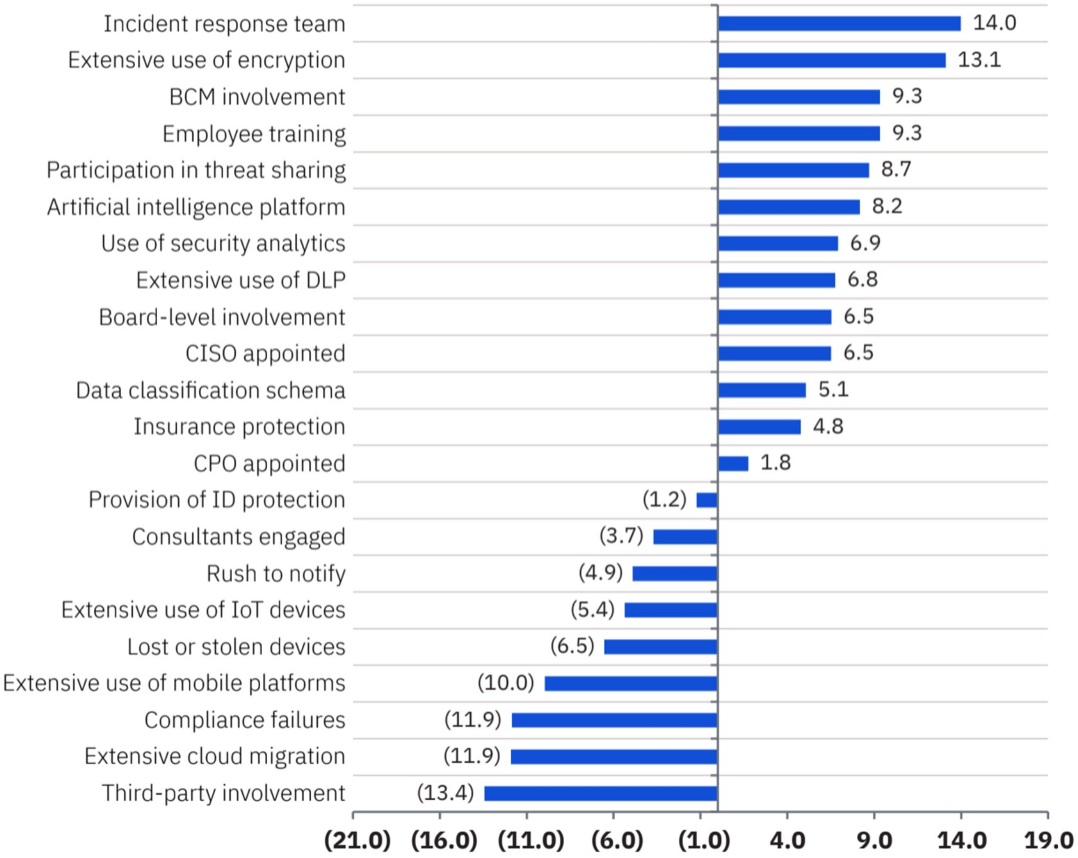
MTTC Comparison



Source: 2018 Cost of Data Breach: Impact of BCM, IBM

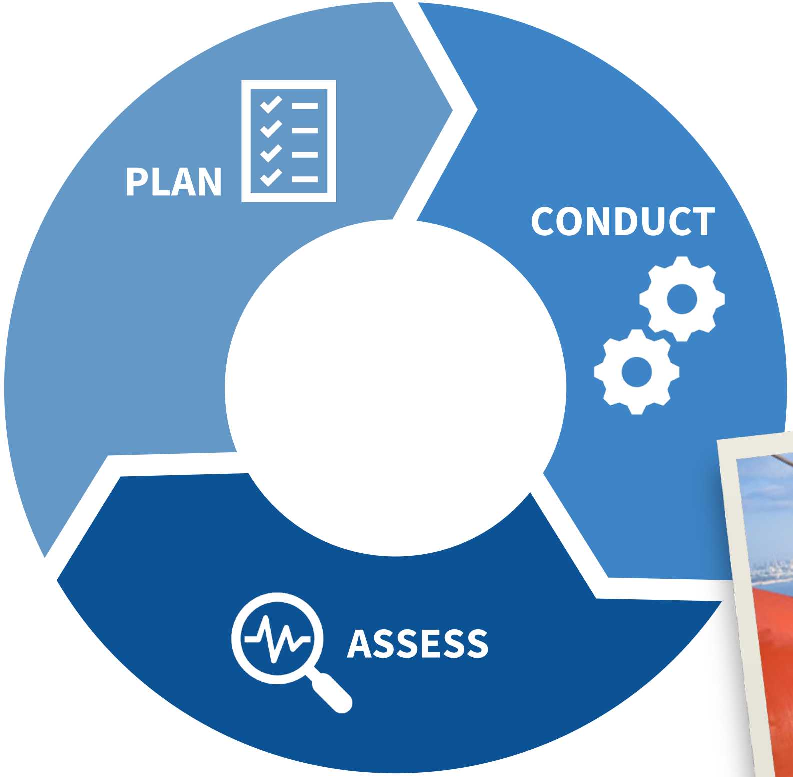
BCM involvement improves Incident Response (COST)

BCM involvement, along with a solid incident response team, reduces the per capita cost of a data breach



Source: 2018 Cost of Data Breach: Impact of BCM, IBM

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

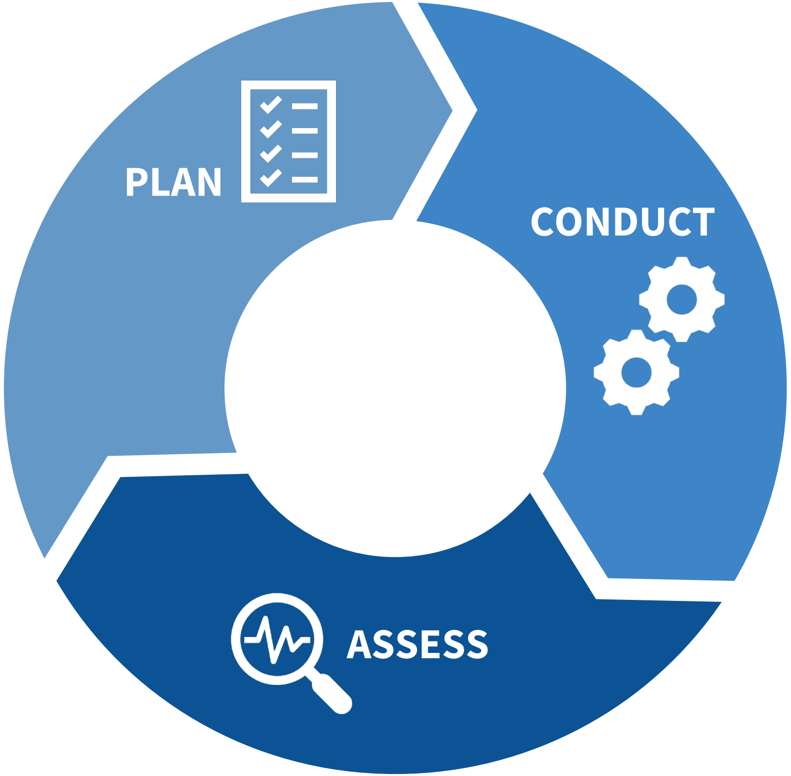
Leverage NIST SP800-61 Computer Security Incident Handling Guide

Must address elements of preparation, detection, analysis, containment, eradication, recovery

You have initial leadership support (with intent of ongoing support)

You have existing tools and processes to detect and report an incident

Recurring Incident Response (IR) Exercise Cycle



PLAN

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

PLAN

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 in exercise
- Gather info and intelligence on areas and groups which may be in scope

PLAN

Narrowing

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

PLAN

Logistics

- Day of week – Monday vs Friday
- Time of day – morning vs afternoon vs through lunch
- 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)

CONDUCT

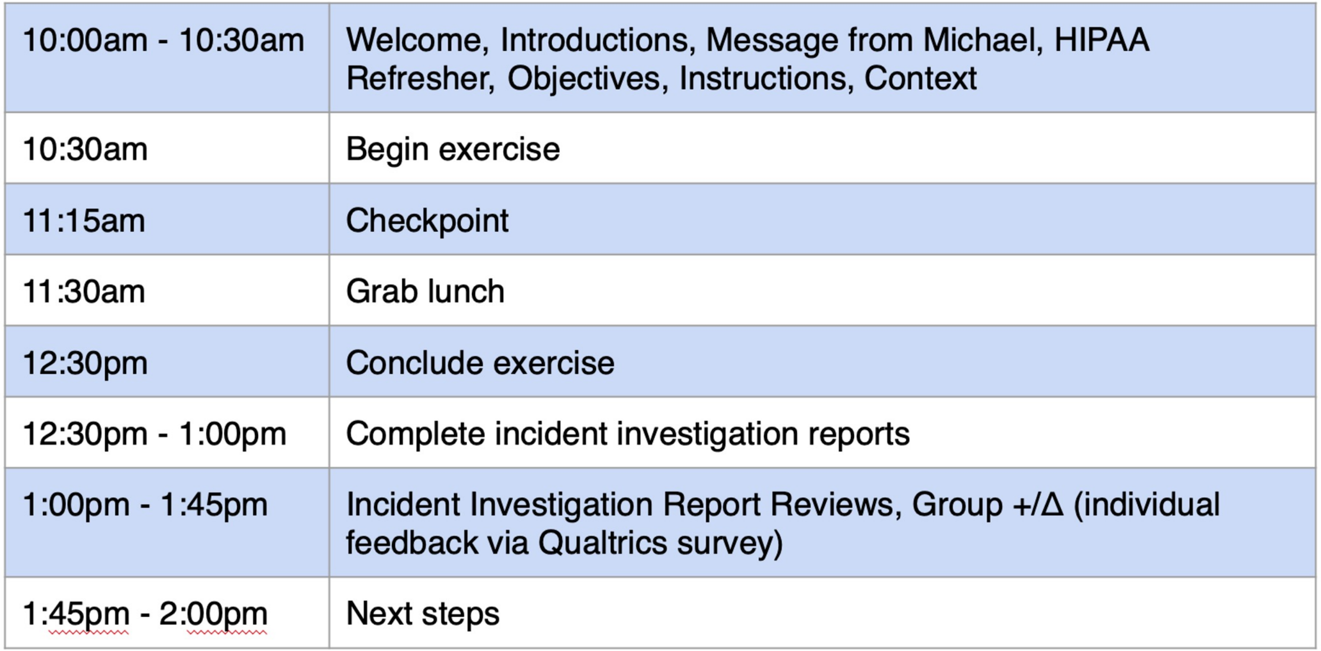
Day of the Exercise:

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

Day of the exercise

CONDUCT

Example Agenda



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

CONDUCT

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!

CONDUCT

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.

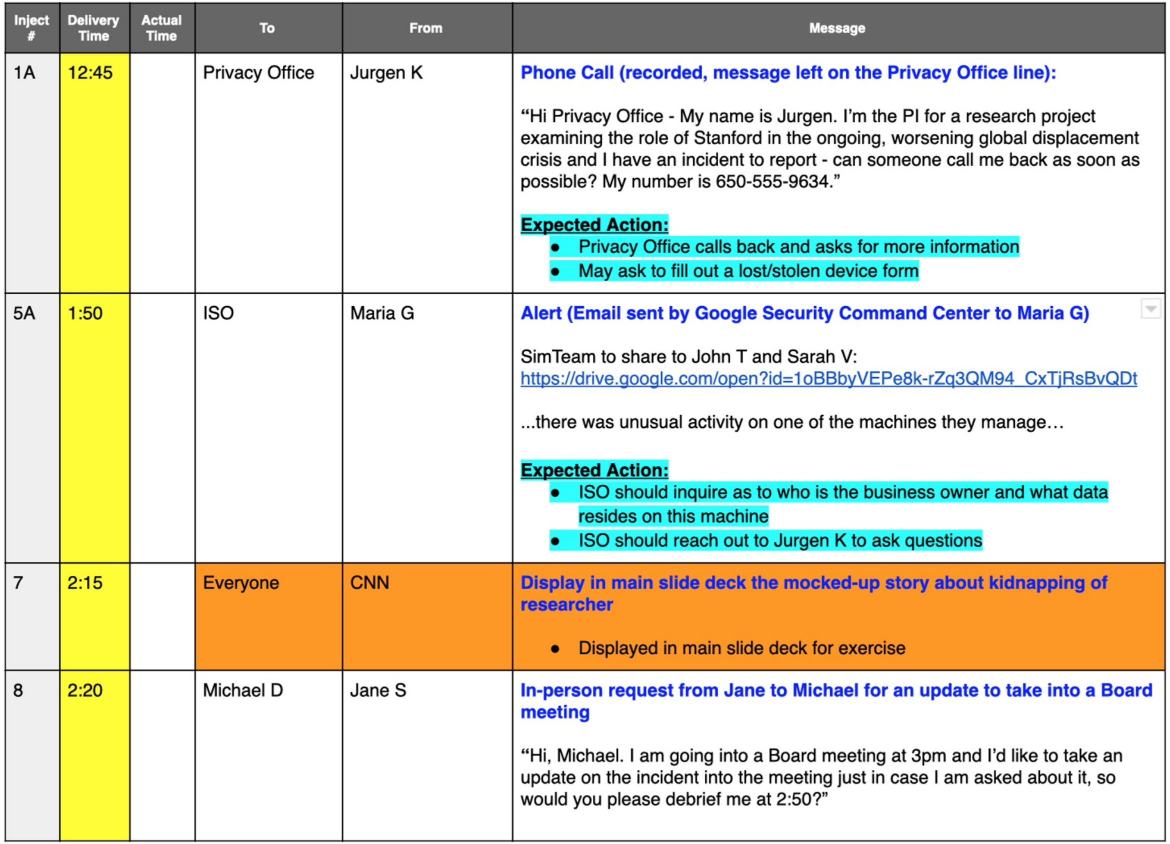
CONDUCT

Example Scenarios

- Lost/Stolen Laptop
- Server infected by ransomware
- DDoS Attack
- Spear phishing campaign
- Website compromise or defacement
- DNS compromise
- Breach that triggers HIPAA notification
- SCADA system compromise
- Digital signage system compromise
- Insider abuse of privileges
- Data breach and exfiltration
- Database breach through malware
- Data exposed in a public cloud service
- User requests “right to be forgotten” per GDPR
- Server compromised and used for crypto-mining
- Transaction application compromise

CONDUCT

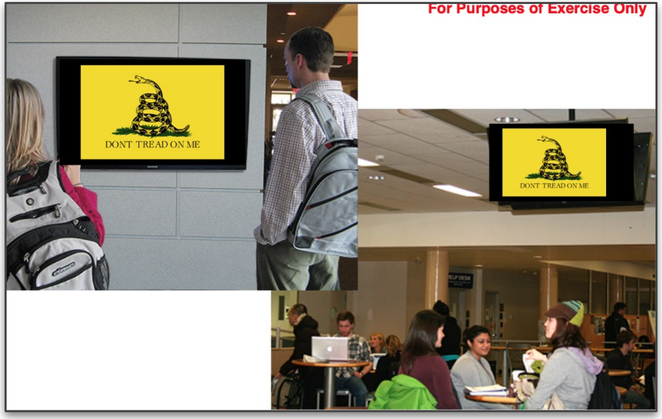
Example Master Scenario Events List (MSEL)



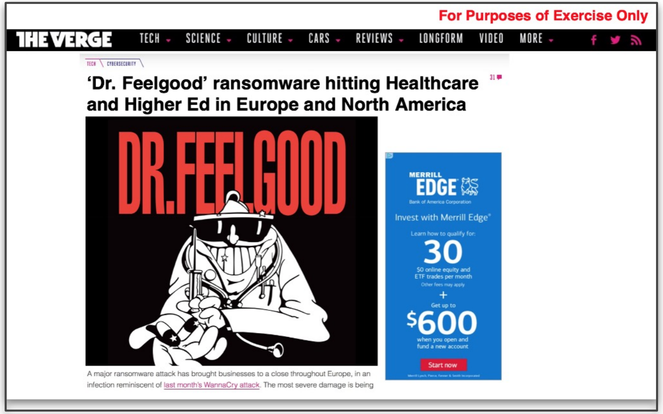
Inject #	Delivery Time	Actual Time	To	From	Message
1A	12:45		Privacy Office	Jurgen K	**Phone Call (recorded, message left on the Privacy Office line):** "Hi Privacy Office - My name is Jurgen. I'm the PI for a research project examining the role of Stanford in the ongoing, worsening global displacement crisis and I have an incident to report - can someone call me back as soon as possible? My number is 650-555-9634." **Expected Action:** ● Privacy Office calls back and asks for more information ● May ask to fill out a lost/stolen device form
5A	1:50		ISO	Maria G	**Alert (Email sent by Google Security Command Center to Maria G)** SimTeam to share to John T and Sarah V: https://drive.google.com/open?id=1oBBbyVEPe8k-rZq3QM94_CxTjRsBvQDt ...there was unusual activity on one of the machines they manage… **Expected Action:** ● ISO should inquire as to who is the business owner and what data resides on this machine ● ISO should reach out to Jurgen K to ask questions
7	2:15		Everyone	CNN	**Display in main slide deck the mocked-up story about kidnapping of researcher** ● Displayed in main slide deck for exercise
8	2:20		Michael D	Jane S	**In-person request from Jane to Michael for an update to take into a Board meeting** "Hi, Michael. I am going into a Board meeting at 3pm and I'd like to take an update on the incident into the meeting just in case I am asked about it, so would you please debrief me at 2:50?"

CONDUCT

Example Injects



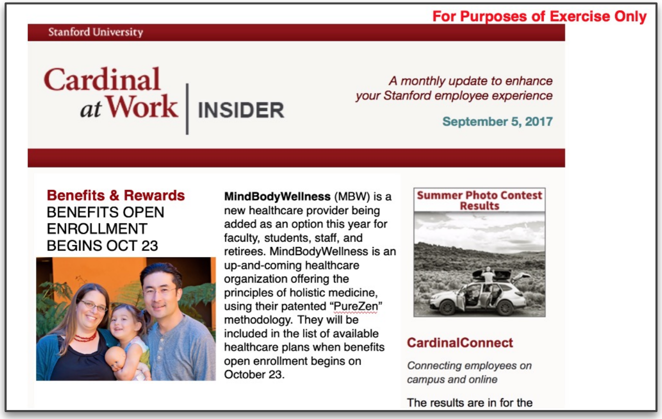
For Purposes of Exercise Only



For Purposes of Exercise Only

‘Dr. Feelgood’ ransomware hitting Healthcare and Higher Ed in Europe and North America

A major ransomware attack has brought businesses to a close throughout Europe, in an infection reminiscent of last month's WannaCry attack. The most severe damage is being



For Purposes of Exercise Only

Stanford University

Cardinal at Work | INSIDER

A monthly update to enhance your Stanford employee experience

September 5, 2017

Benefits & Rewards

BENEFITS OPEN ENROLLMENT BEGINS OCT 23

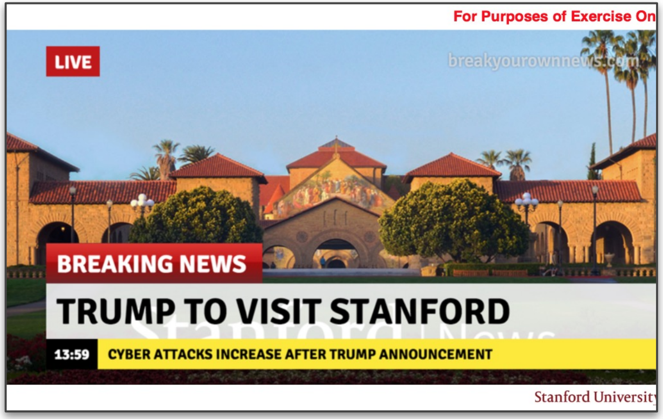
MindBodyWellness (MBW) is a new healthcare provider being added as an option this year for faculty, students, staff, and retirees. MindBodyWellness is an up-and-coming healthcare organization offering the principles of holistic medicine, using their patented “PureZen” methodology. They will be included in the list of available healthcare plans when benefits open enrollment begins on October 23.

Summer Photo Contest Results

CardinalConnect

Connecting employees on campus and online

The results are in for the



For Purposes of Exercise On

LIVE

breakyourownnews.com

BREAKING NEWS

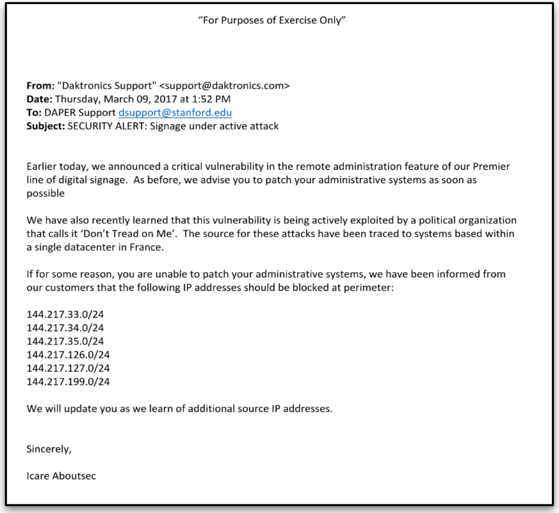
TRUMP TO VISIT STANFORD

13:59 CYBER ATTACKS INCREASE AFTER TRUMP ANNOUNCEMENT

Stanford University

CONDUCT

Example Injects



"For Purposes of Exercise Only"

From: "Daktronics Support" <support@daktronics.com>
Date: Thursday, March 09, 2017 at 1:52 PM
To: DAPER Support dsupport@stanford.edu
Subject: SECURITY 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 Tread on Me'. The source for these attacks have been traced to systems based within a single datacenter in France.

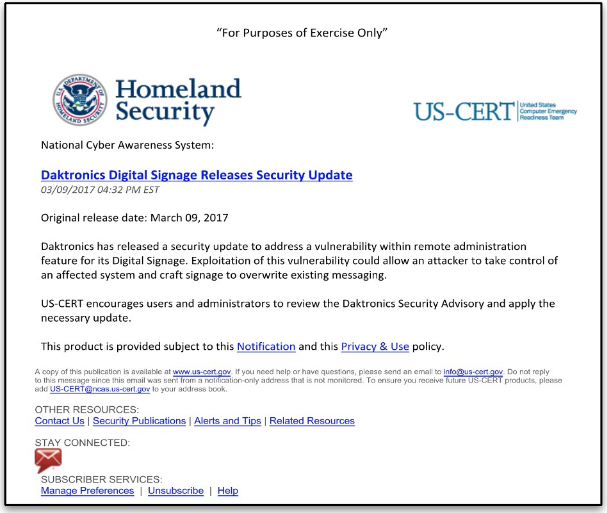
If for some reason, you are unable to patch your administrative systems, we have been informed from our customers that the following IP addresses should be blocked at perimeter:

144.217.33.0/24
144.217.34.0/24
144.217.35.0/24
144.217.126.0/24
144.217.127.0/24
144.217.199.0/24

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

Sincerely,

Icare Aboutsec



"For Purposes of Exercise Only"

Homeland Security

US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

Daktronics Digital Signage Releases Security Update
03/09/2017 04:32 PM EST

Original release date: March 09, 2017

Daktronics has released a security update to address a vulnerability within remote administration feature for its Digital Signage. Exploitation of this vulnerability could allow an attacker to take control of an affected system and craft signage to overwrite existing messaging.

US-CERT encourages users and administrators to review the Daktronics Security Advisory and apply the necessary update.

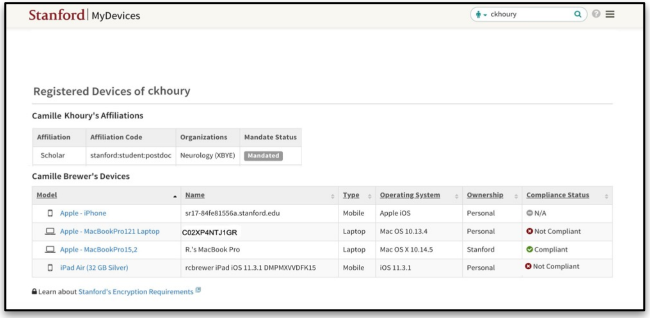
This product is provided subject to this Notification and this Privacy & Use policy.

A copy of this publication is available at www.us-cert.gov. If you need help or have questions, please send an email to info@us-cert.gov. Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:
Contact Us | Security Publications | Alerts and Tips | Related Resources

STAY CONNECTED:

SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help



Registered Devices of ckhoury

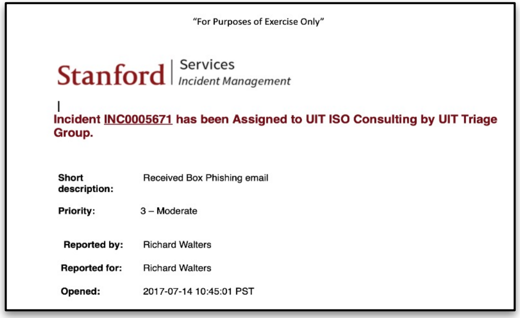
Camille Khoury's Affiliations

Affiliation	Affiliation Code	Organizations	Mandate Status
Scholar	stanford:student:postdoc	Neurology (XBYE)	Mandated

Camille Brewer's Devices

Model	Name	Type	Operating System	Ownership	Compliance Status
Apple - iPhone	sr17-84fe81556a.stanford.edu	Mobile	Apple iOS	Personal	N/A
Apple - MacBookPro121 Laptop	C02XP4NTJ1GR	Laptop	Mac OS 10.13.4	Personal	✗ Not Compliant
Apple - MacBookPro15,2	R.'s MacBook Pro	Laptop	Mac OS X 10.14.5	Stanford	✓ Compliant
iPad Air (32 GB Silver)	rcbrewer iPad iOS 11.3.1 DMPMXVVDFK15	Mobile	iOS 11.3.1	Personal	✗ Not Compliant

Learn about Stanford's Encryption Requirements



"For Purposes of Exercise Only"

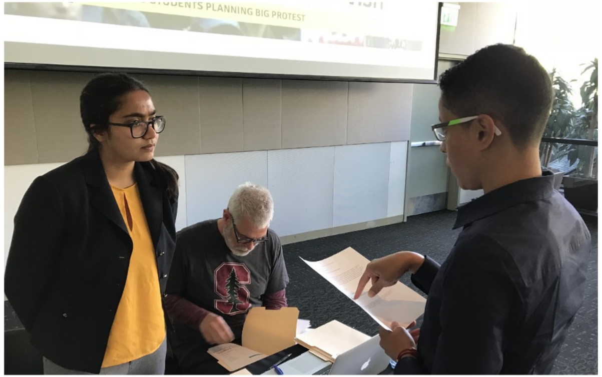
Stanford | Services
Incident Management

Incident INC0005671 has been Assigned to UIT ISO Consulting by UIT Triage Group.

Short description:	Received Box Phishing email
Priority:	3 – Moderate
Reported by:	Richard Walters
Reported for:	Richard Walters
Opened:	2017-07-14 10:45:01 PST

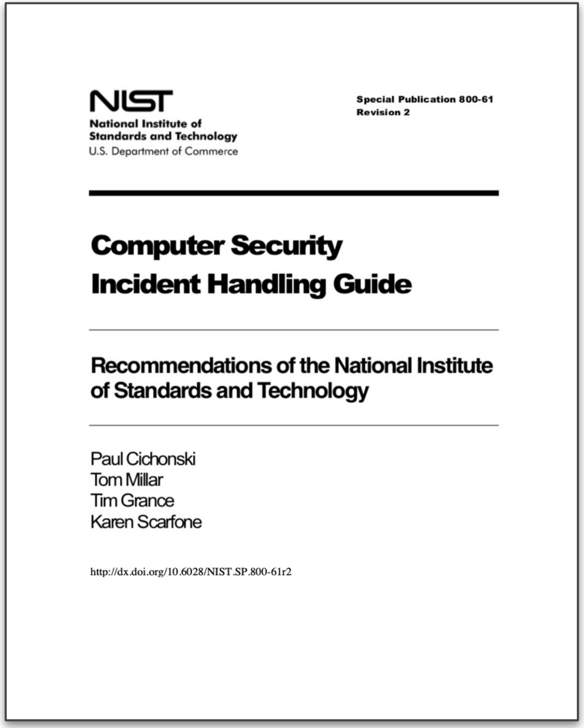
CONDUCT

Example Injects



Life on the border: Stanford researcher seeks to help Syrian refugees

CONDUCT Option: Leverage existing scenarios and situation manuals



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

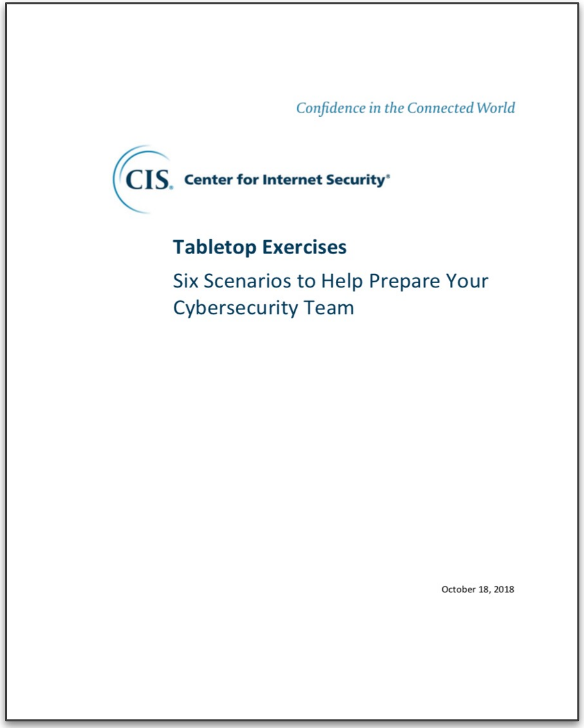
Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2



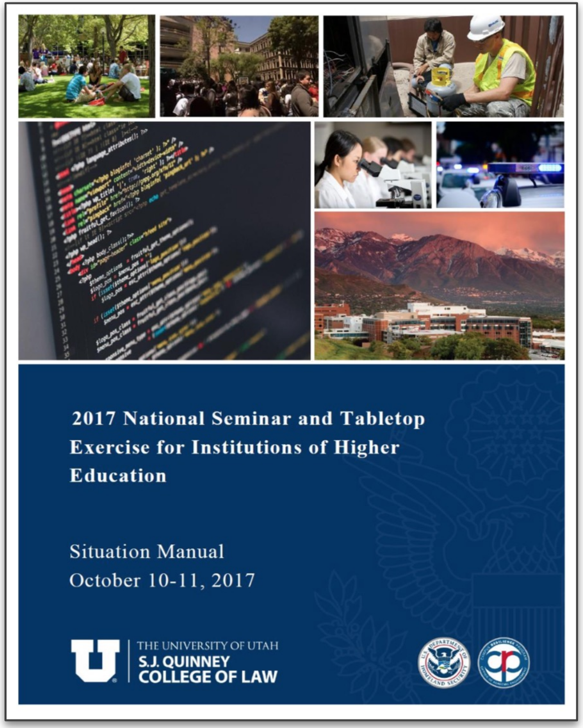
Confidence in the Connected World

CIS. Center for Internet Security®

Tabletop Exercises

Six Scenarios to Help Prepare Your Cybersecurity Team

October 18, 2018



2017 National Seminar and Tabletop Exercise for Institutions of Higher Education

Situation Manual
October 10-11, 2017

THE UNIVERSITY OF UTAH
S.J. QUINNEY
COLLEGE OF LAW

CONDUCT Option: Hold a “distributed only” exercise

CONDUCT Option: Record your “report-outs” for later review

Information Security Office
security.stanford.edu
Stanford | University IT
encrypt.stanford.edu
dataclass.stanford.edu
minsec.stanford.edu

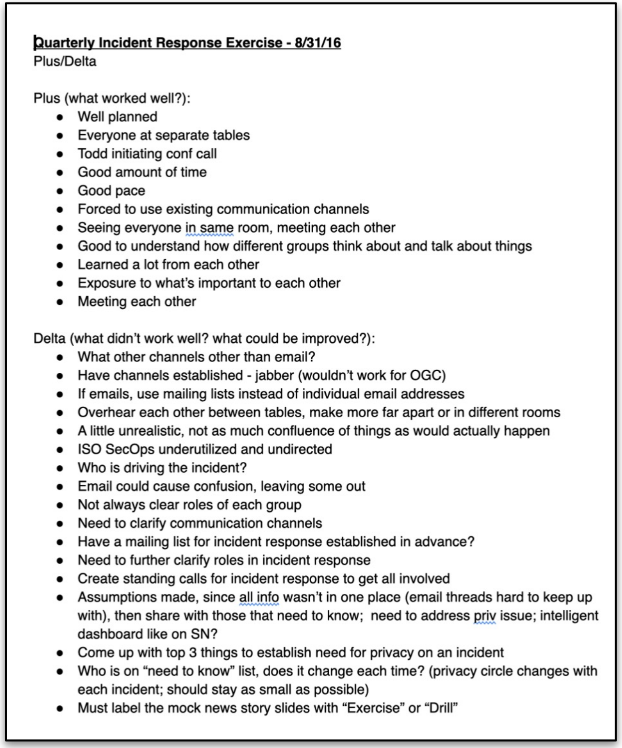
ASSESS

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

ASSESS

Gathering Group Feedback



Quarterly Incident Response Exercise - 8/31/16

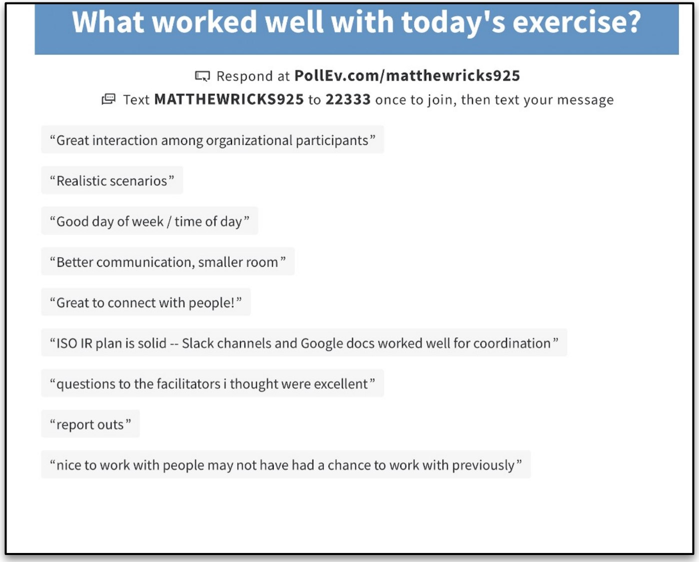
Plus/Delta

Plus (what worked well?):

- 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 OGC)
- 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 place (email threads hard to keep up with), then share with those that need to know; need to address priv issue; intelligent dashboard like on SN?
- 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?

Respond at **PollEv.com/matthewricks925**

Text **MATTHEWRICKS925** to **22333** once to join, then text your message

"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"

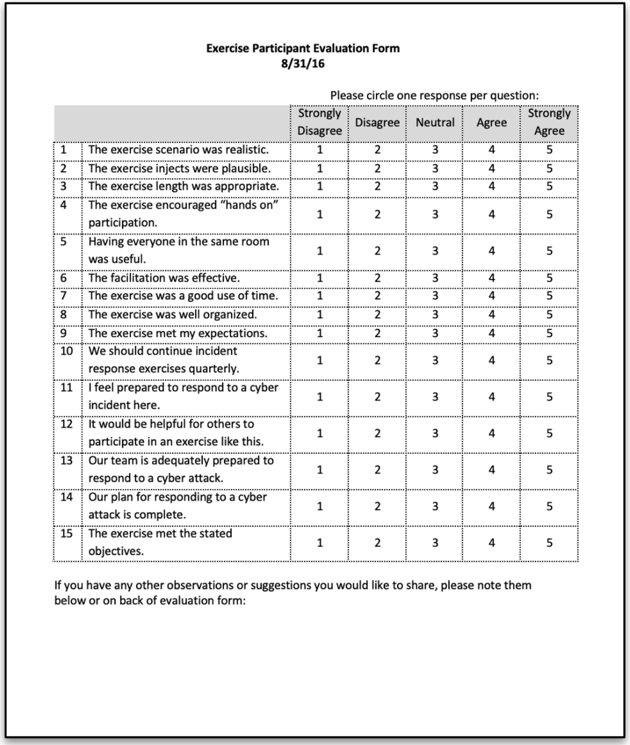
"questions to the facilitators i thought were excellent"

"report outs"

"nice to work with people may not have had a chance to work with previously"

ASSESS

Gathering Individual Feedback



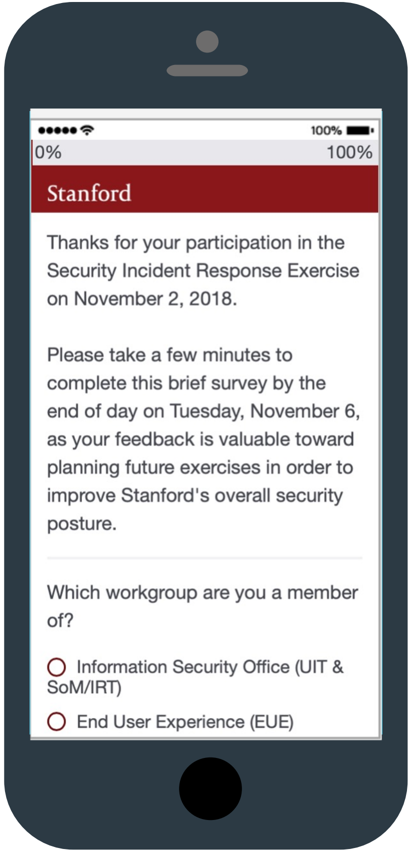
Exercise Participant Evaluation Form
8/31/16

Please circle one response per question:

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

If you have any other observations or suggestions you would like to share, please note them below or on back of evaluation form:

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



Stanford

Thanks for your participation in the Security Incident Response Exercise on November 2, 2018.

Please take a few minutes to complete this brief survey by the end of day on Tuesday, November 6, as your feedback is valuable toward planning future exercises in order to improve Stanford's overall security posture.

Which workgroup are you a member of?

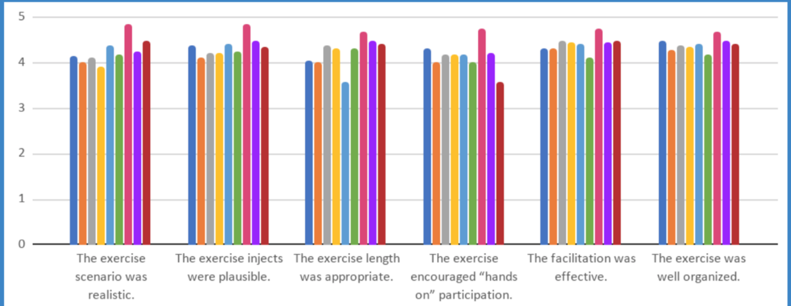
○ Information Security Office (UIT & SoM/IRT)

○ End User Experience (EUE)

ASSESS

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.



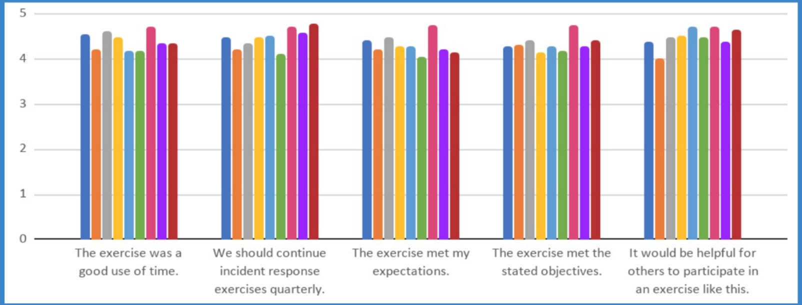
5-point survey rating scale:

5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree

ASSESS

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.



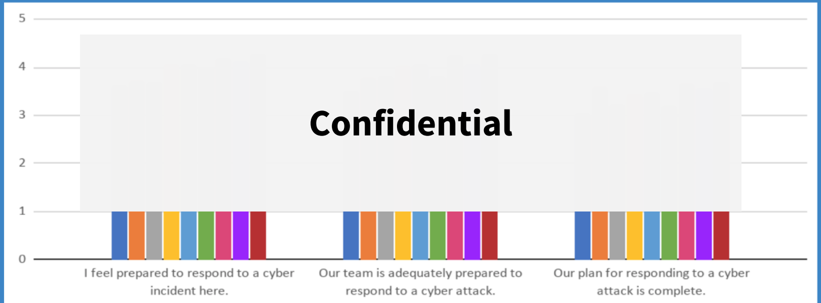
5-point survey rating scale:

5 = Strongly Agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly Disagree

ASSESS

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 responses

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

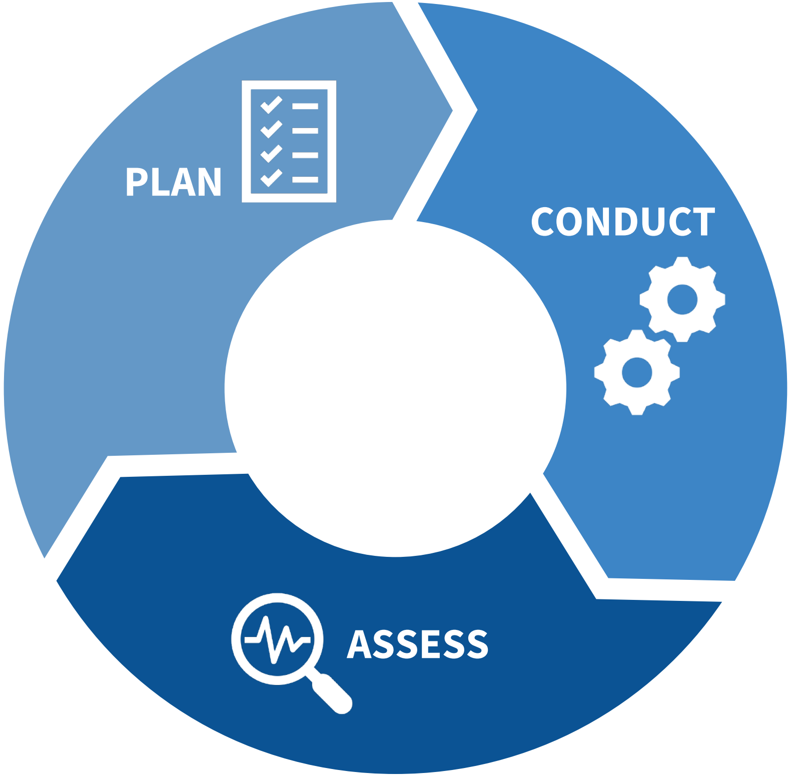
How it all comes together…

https://youtu.be/_5rbBYhwW1k

What have you done to improve incident response capabilities within your own organizations?

Call to Action

- Extend the partnership between BCM and your Information Security Office
- 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

Stanford University

University IT (UIT)

October 2019