### GRACE HOPPER CELEBRATION



## Wargames and Tabletops

How to Get Everyone from Your Board of Directors to your Analyst Ready for a Cyber Security Incident about me



### A day in the life ...

4:00 pm



Malware is detected on a machine after a user clicks an email link

Reimage and educate

5:00 pm



Investigation shows the email appears to have come from a vendor

Alert vendor

7:00 pm



Vendor reveals they are investigating a potentially significant breach

... Now what!?

### What do you do next?

- How can I cut vendor access?
- How will my decisions impact operations?
- How can I minimize impact to our guests?
- What should I be prepared to say externally?
- Will this trigger regulatory or reporting requirements?

... and how do we coordinate everything in this time of crisis?

At Target, Enterprise Incident Management is a structured process, escalation, and decision framework that allows the technical team to stay focused on technical investigation and containment

### Agenda



Pick the right people.

Form a cross-functional core team of 5-7



Process over plan

Agree before the incident occurs



Practice, Practice, Practice

Must represent their function + the company

# Create a severity framework, not calculator



Risk to a large quantity of sensitive information, extreme disruption to business operations or threat to human safety.

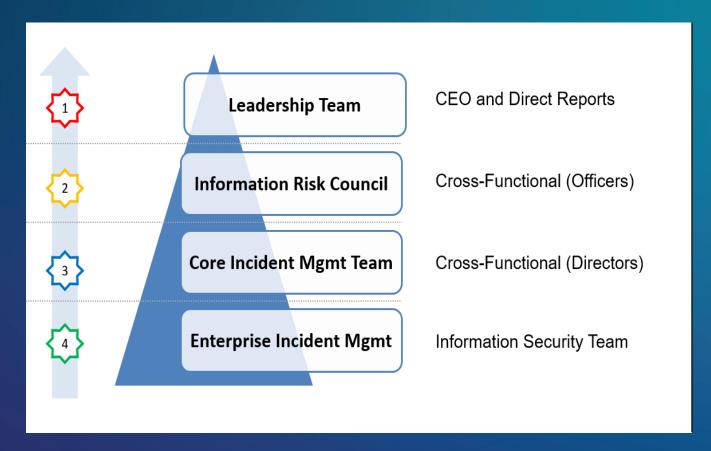
Risk to a moderate quantity of sensitive information or significant disruption to business operations.

Risk to a low quantity of sensitive information or moderate disruption to business operations.

No risk to sensitive information and minimal disruption to business operations

### **Target Example**

#### **Severity Escalation**



#### **Team Representatives**

- ✓ Information Security
- ✓ Legal
- **✓** Communications
- ✓ Fraud
- ✓ Physical Security
- ✓ Financial Services

### War Room



# Define the process rather than a "plan"

1. Triage & Contain

2. Investigate & Recover

3. Post-Incident Analysis

Event is identified & short-term containment is in place



Facts of event are determined for remediation



Event recovery & long-term remediation



Lessons learned are documented

- \_\_\_\_
- Assess initial event details
   Assign initial severity
- Based on severity triggers, determine if CIMT and/or IRC need to be engaged
- · Engage appropriate SMEs
- Ensure short-term containment actions completed

- · Investigate full event details to reassess scope & severity
- Engage broader support teams as needed and assign response and remediation activities
- Ensure long-term remediation activities are completed
- Execute communication and public relations plans, ensuring a consistent message across all channels
- Execute notifications obligations to individuals, regulatory agencies, and third parties, if applicable
- Obtain applicable approvals from the IRC and/or LT R&R as necessary

- · Conduct lessons learned
- Update processes and procedures based on post-incident analysis
- Ensure any ongoing post-close remediation activities have been assigned
- Close out all case documentation

Information Risk Council

Management Team

Core Incident

 Informed of the event by the CIMT, based on severity
 Provide input into the

- Provide input into the response and containment activities, as needed
- Determine if further escalation is required

- Provide input into the investigation and long-term remediation plans
- Provide input into the communication and public relations plans
- · Provide input into the notification obligations
- Ensure all activities are properly executed to approve the case to move to the post-incident analysis phase

 Participate in lessons learned to drive further program enhancements as applicable

Leadership Team Risk & Reputation

Tools

- · Informed of the event by the IRC, based on severity
- · Determine if further escalation is required
- Approve the strategy and associated response activities developed by IRC and CIMT
- Review and approve all key decisions escalated by the IRC
- Review remediation activities escalated by the IRC
- · Review and comment on communication plans and notification obligations
- EIM Plan
- · EIM Severity Grid
- · Internal Escalation Model

- Communication Guidelines
- Notification Guide
- SME Contact List

- Case Activity Timeline Tracker
- CIMT and IRC Incident Checklists
- Event Notification

### War Room



Ditch the templates for a whiteboard



### Year 1: Getting Started

Prepares the company for when defenses fail by simulating a significant security event

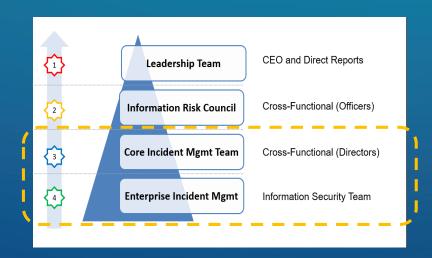


Scenario Complexity

POS Breach

Focus Area (Train and Test)

"Boots on the ground"



The following video is part of a fictional scenario to be used for wargame purposes only

### Year 2: Intermediate

We elevated the level of realism, surprise and Leadership Team dependencies





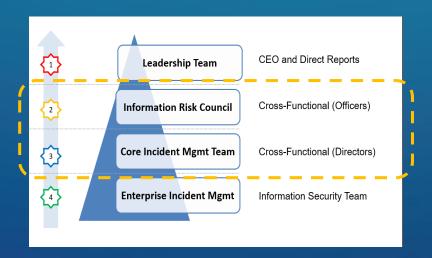
POS Breach Insider Threat



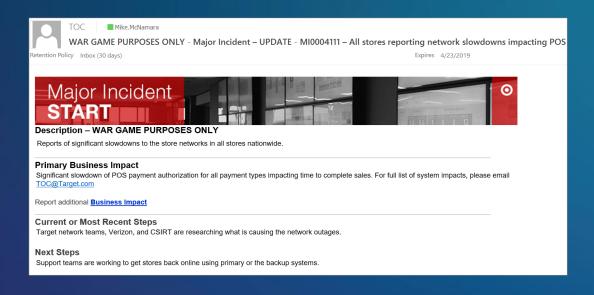
"Boots on the ground" Officer Teams



CISO unreachable

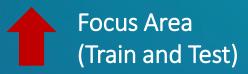


### Year 3: Advanced





Insider Threat
Ransom and Operations

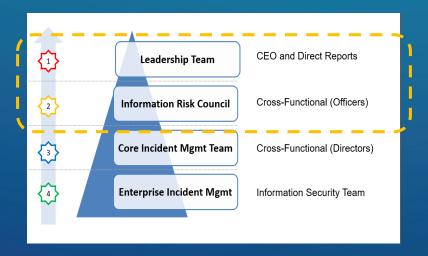


Officer Teams
CEO & Staff



Unexpected twists

Surprise!



### Things to remember

Independent
observation will drive
more meaningful
feedback

Debrief lessons learned while everyone is still in game mode Create meaningful action plans to drive continuous improvement

### War Room



### Takeaways



Create a core team of trusted partners



**Keep it Simple!** 



Effective wargames feel "almost too real"

### Thank you!

Please remember to complete the session survey in the mobile app.

