

GRACE HOPPER CELEBRATION



ANITA
B.ORG

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

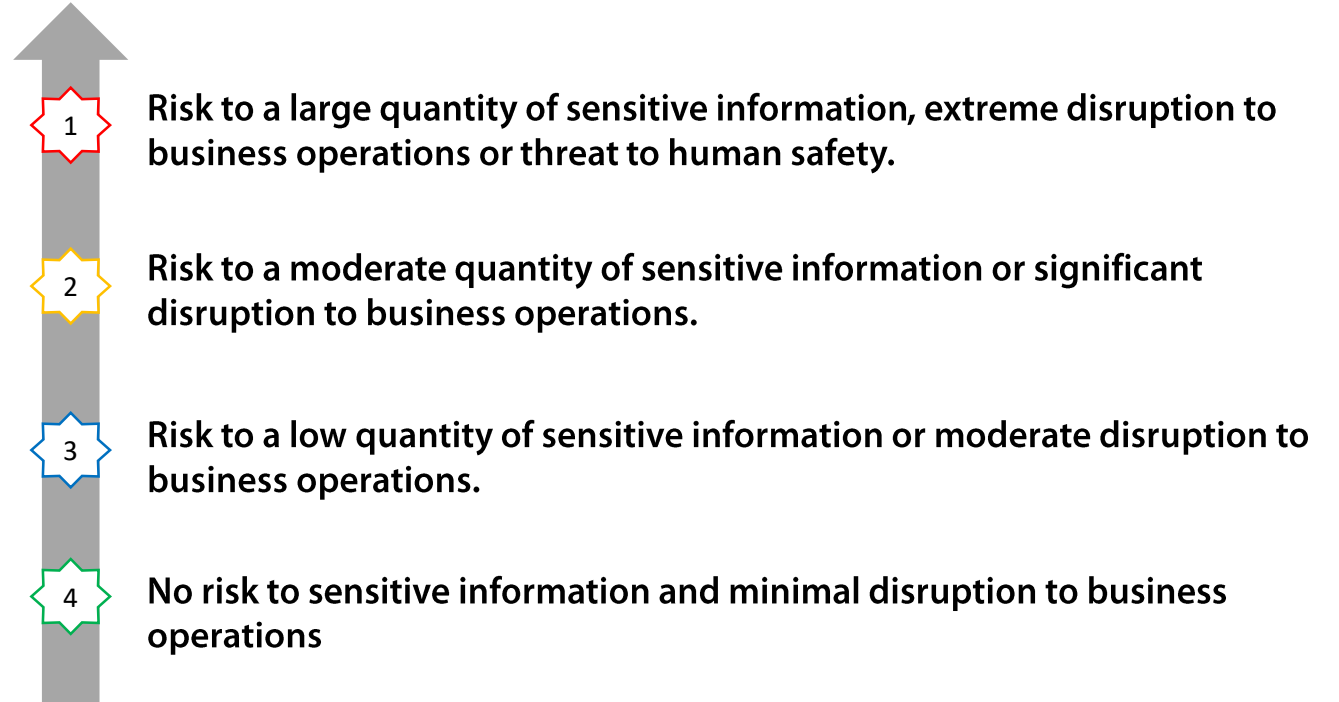
Agree before the incident occurs



Practice, Practice, Practice

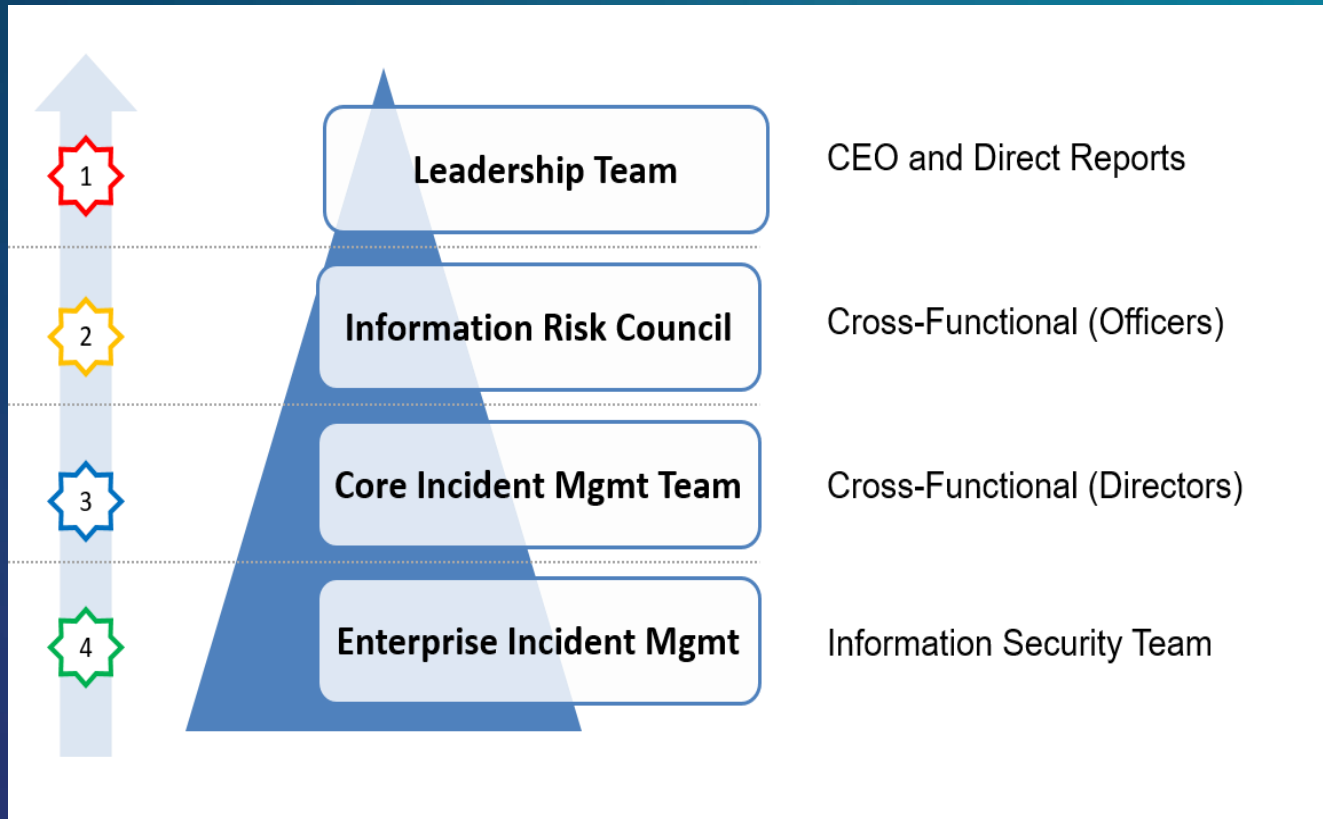
Must represent their function + the company

Create a severity framework, not calculator



Target Example

Severity Escalation



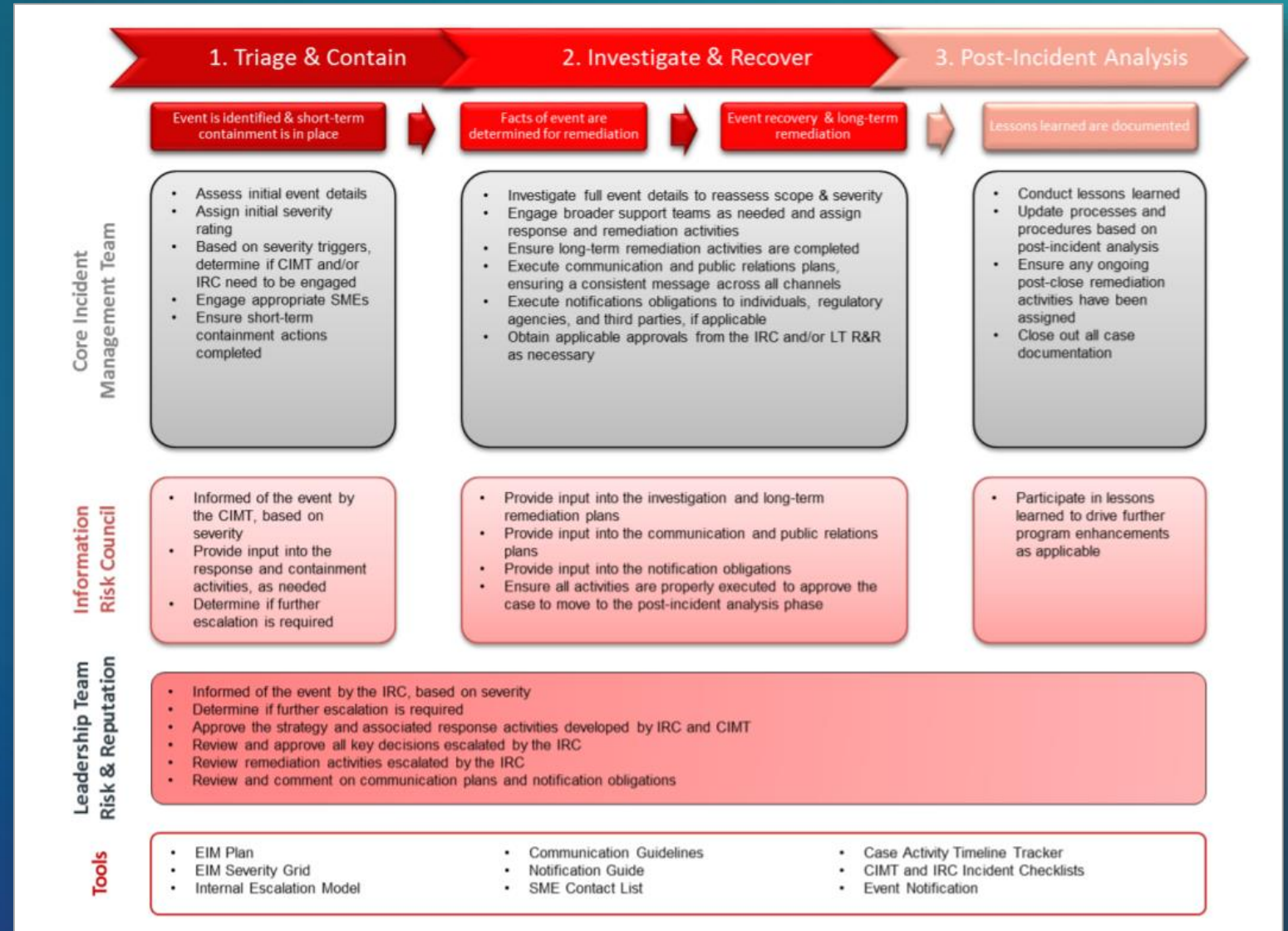
Team Representatives

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

War Room



Define the process rather than a “plan”



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*

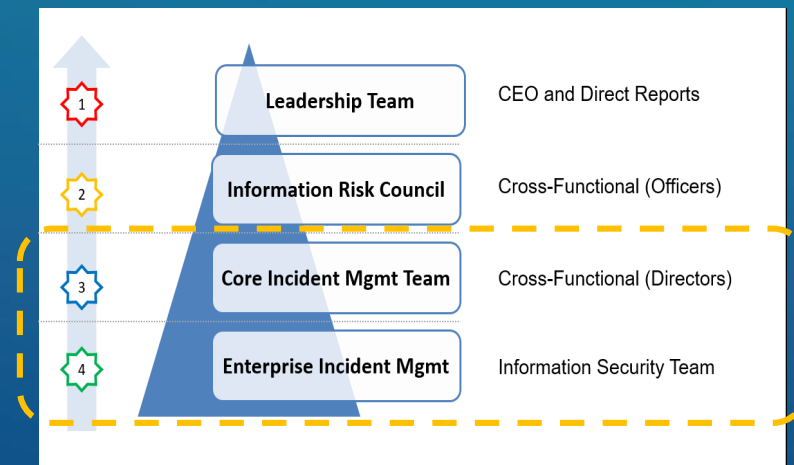


Scenario
Complexity

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



Scenario Complexity

POS Breach
Insider Threat



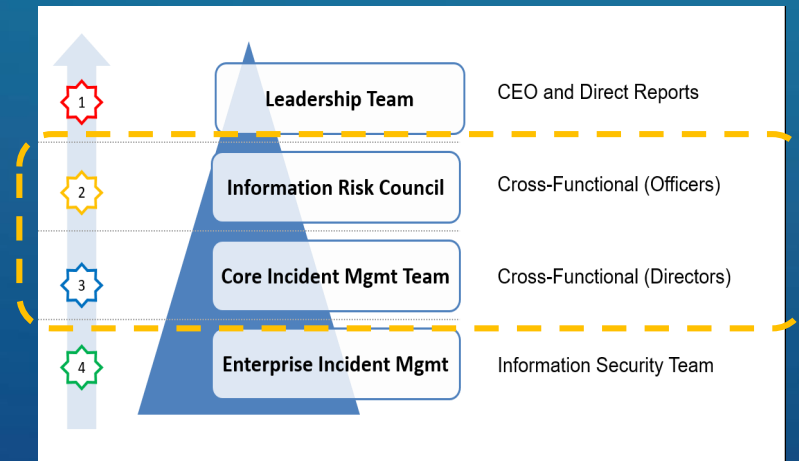
Focus Area
(Train and Test)

"Boots on the ground"
Officer Teams



Unexpected twists

CISO unreachable




Year 3: Advanced

TOC | Mike.McNamara

WAR GAME PURPOSES ONLY - Major Incident – UPDATE - MI0004111 – All stores reporting network slowdowns impacting POS

Retention Policy | Inbox (30 days) | Expires 4/23/2019



Description – WAR GAME PURPOSES ONLY
Reports of significant slowdowns to the store networks in all stores nationwide.

Primary Business Impact
Significant slowdown of POS payment authorization for all payment types impacting time to complete sales. For full list of system impacts, please email TOC@Target.com

Report additional [Business Impact](#)

Current or Most Recent Steps
Target network teams, Verizon, and CSIRT are researching what is causing the network outages.

Next Steps
Support teams are working to get stores back online using primary or the backup systems.



Scenario
Complexity

Insider Threat
Ransom and Operations



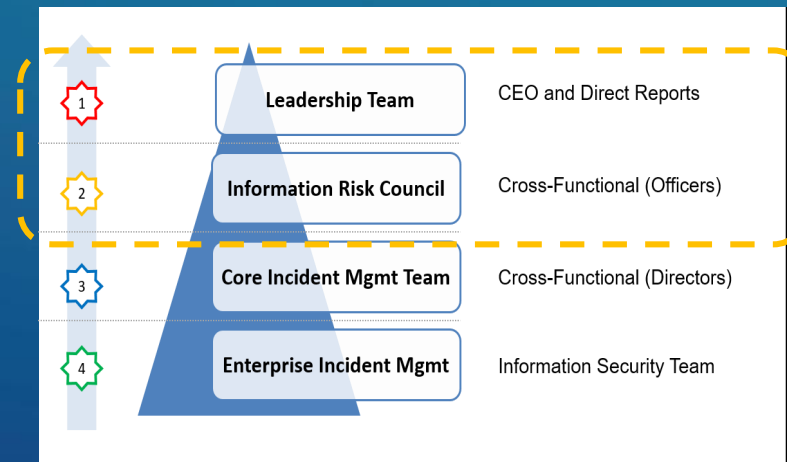
Focus Area
(Train and Test)

Officer Teams
CEO & Staff



Unexpected
twists

Surprise!



For Wargame Purposes Only

#GHC19

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.

GRACE HOPPER
CELEBRATION



#GHC19