RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

RSAConference2020

HUMAN ELEMENT

SESSION ID: AIR-T08

How to prepare everyone for a Crisis?

Erin Becker

Director, Enterprise Incident Management
Target

The world we live in…

RSAConference2020 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!?

"Example Only"

What do you do next?

- How can I minimize impact to our guests?
- What should I be prepared to say externally?
- How will my decisions impact operations?
- 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

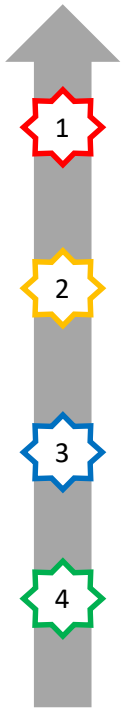
Agenda

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

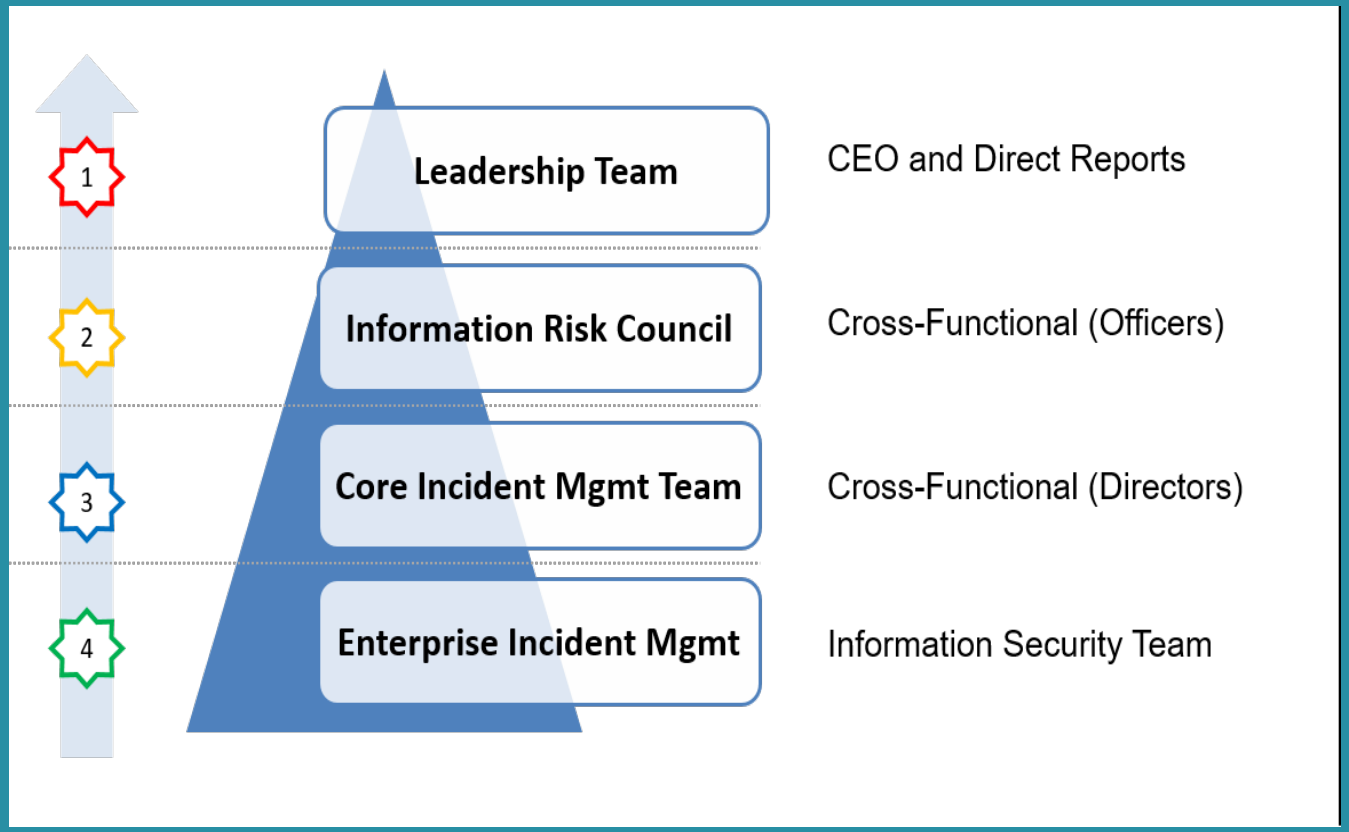
Create a severity framework, not calculator



1. **Risk to a large quantity of sensitive information, extreme disruption to business operations or threat to human safety.**
2. **Risk to a moderate quantity of sensitive information or significant disruption to business operations.**
3. **Risk to a low quantity of sensitive information or moderate disruption to business operations.**
4. **No risk to sensitive information and minimal disruption to business operations**

Target Example

Severity Escalation



Team Representatives

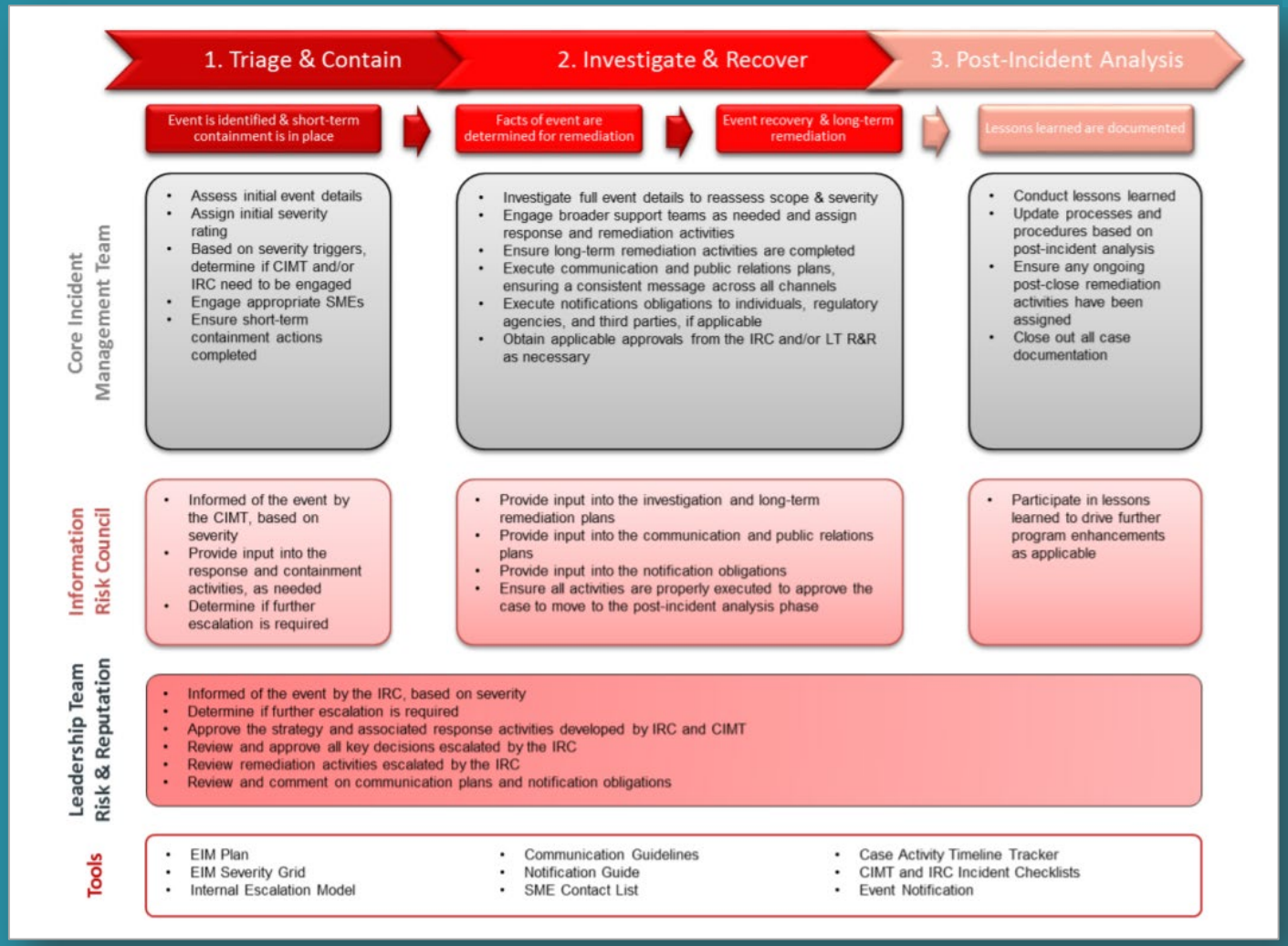
- V Information Security
- V Legal
- V Public Relations
- V Fraud
- V Physical Security
- V Financial Services

War Room

You have all the right people activated in the war room…

Now What?

Define the process rather than a “plan”



War Room

There is a lot happening in the war room…

How do you track it all?

How do you communicate up and out?

Ditch the templates for a whiteboard

Year 1: Getting Started

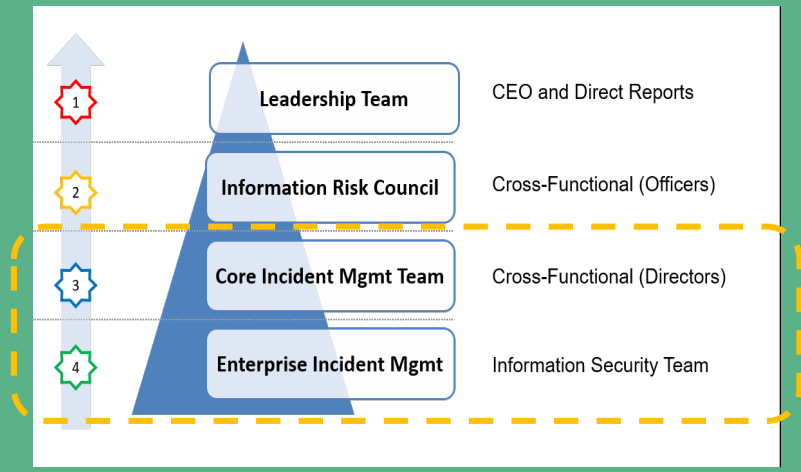
Prepares the company for when defenses fail by simulating a significant security event

Scenario Complexity

POS Breach

Focus Area (Train and Test)

"Boots on the ground"



Year 2: Intermediate

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

Scenario Complexity

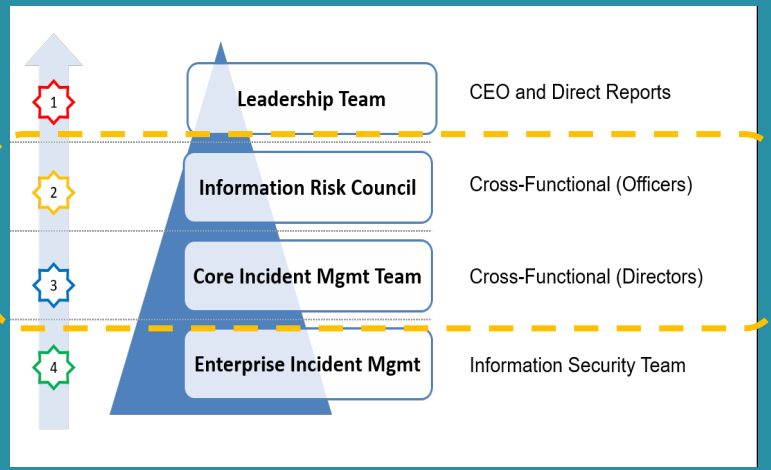
POS Breach
Insider Threat

Focus Area (Train and Test)

"Boots on the ground"
Officer Teams

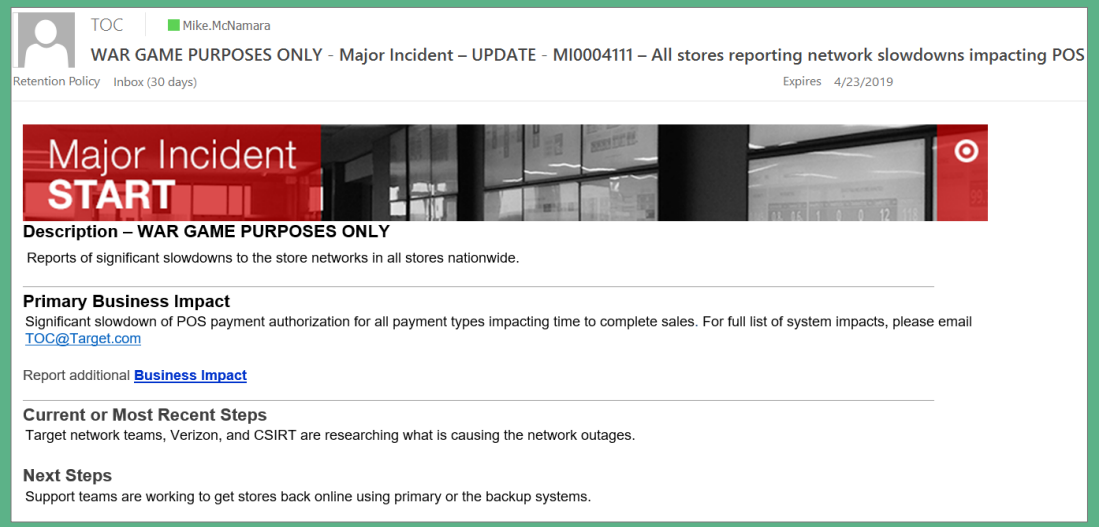
Unexpected twists

CISO unreachable



For Wargame Purposes Only

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

Major Incident START

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**

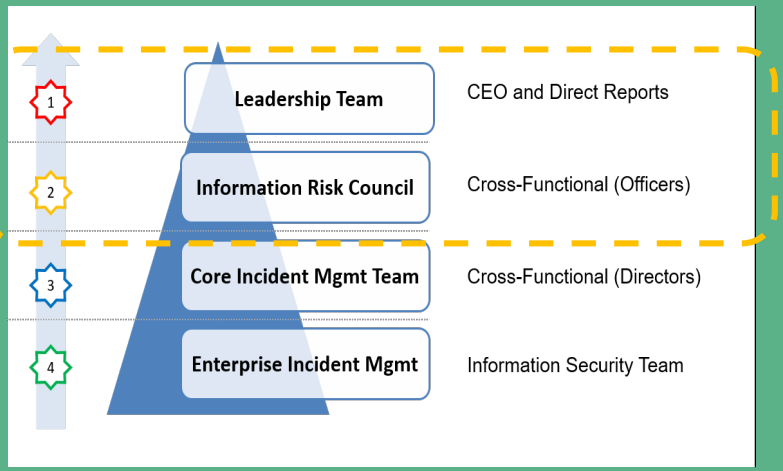
Current or Most Recent Steps

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

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

Takeaways

1. Create a core team of trusted partners
2. Keep it Simple!
3. Effective wargames feel “almost too real”