Deloitte.

PA TechCon

Cyber Wargaming:
You’ve been breached: Now what?

April 26, 2016

Cyber attacks are on the rise

$3.79M

The average cost of a cyber incident[1]

$154

Globally, the average per-record cost of data breach is [1]…

50%

recipients open emails and click on phishing links within the first hour of receiving them [2]

15% of incidents still take days to discover[2]

55% of incidents involve abuse of privileged access[2]

99.9%

of the exploited vulnerabilities were compromised more than a year after CVE* was published [2]

of breaches are not caused by attackers [4]

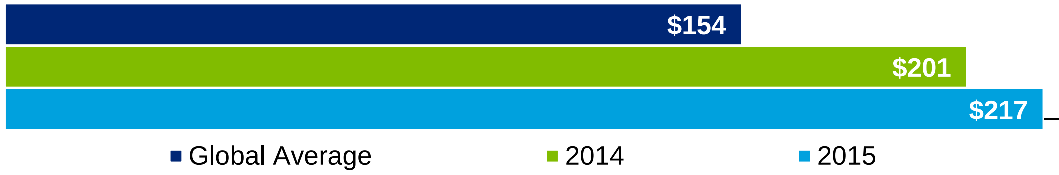
51%

229

Average number of days attackers maintained presence after infiltration and before detection [5]

Per capita cost of data breach was highest in US in 2015 [6]

$217



[1] Ponemon Institute 2015 Cost of Data Breach Study: Global Analysis, May 2015; [3] 2015 Data Breaches: Identity Theft Resource Center Breach Report Hits Near Record High in 2015; [4] April 2015 Symantec ISTR 20 Internet Security Threat Report; [5] Mandiant -Trends® 2014: Beyond the Breach, published April 10, 2014; [6] Ponemon 2015 Cost of Data Breach Study: Global Analysis

Deloitte Advisory's perspective on wargaming

Cyber wargaming is an **interactive technique** that **immerses** potential cyber-incident responders in a **simulated cyber scenario** to help organizations evaluate their **cyber incident response preparedness**

Cyber wargames leverage educational science to:

- Raise awareness of cyber risks, response plans, and capabilities
- Build cohesion among likely cyber incident responders
- Test new cyber incident response strategies in a safe environment
- Expose gaps in people, processes, and technology
- Highlight key cyber incident response dependencies
- Build consensus and a shared vision of cyber incident response

Wargames lead to deeper, broader lessons learned as compared to traditional cyber assessments and tabletop exercises

Agenda

Prebrief

1:15PM – 1:25PM

10 minutes

Wargame

1:25PM – 1:50PM

25 minutes

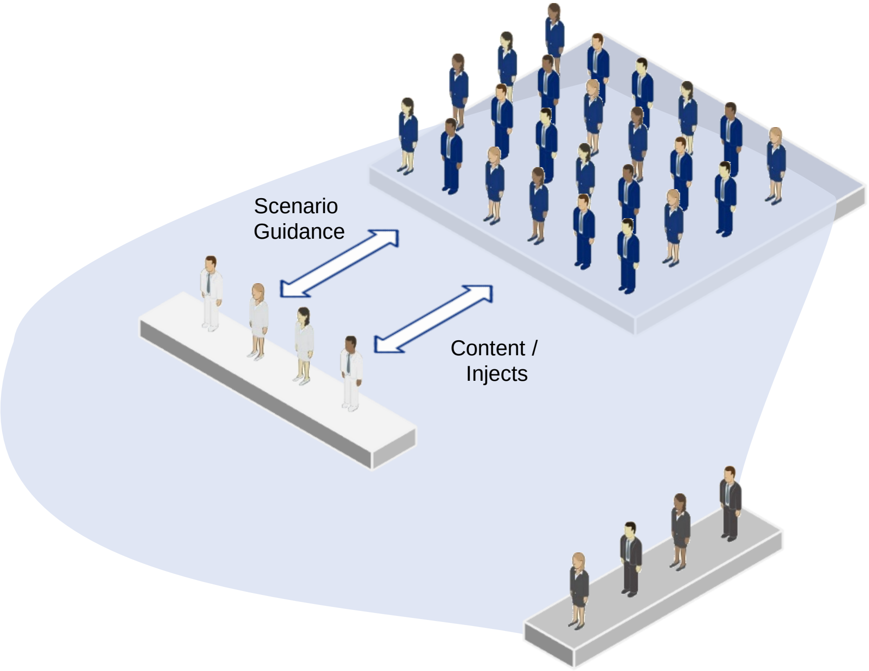
Debrief

1:50PM – 2:00PM

10 minutes

Introduction

Cyber wargaming is an interactive technique that **immerses potential cyber incident responders** in a **simulated cyber scenario** to help organizations evaluate their preparedness to respond to a cyber attack



Incident Responders
Blue Team

Likely cyber incident responders react to exercise injects

Facilitators
White Team

Wargaming specialists manage the direction, pace, and content of the exercise

Observers
Grey Team

Stakeholders observe player actions and decisions

Objectives

1. Establish, maintain, and coordinate command and control during a cyber incident

2. Effectively manage communications both internally and externally

3. Understand the types of processes, plans, and tools that are needed to effectively respond to a cyber incident

How to play

After receiving an inject...

- Review the inject content in its entirety
- Determine what actions you will take and/or what decisions you will make
- Involve others as appropriate

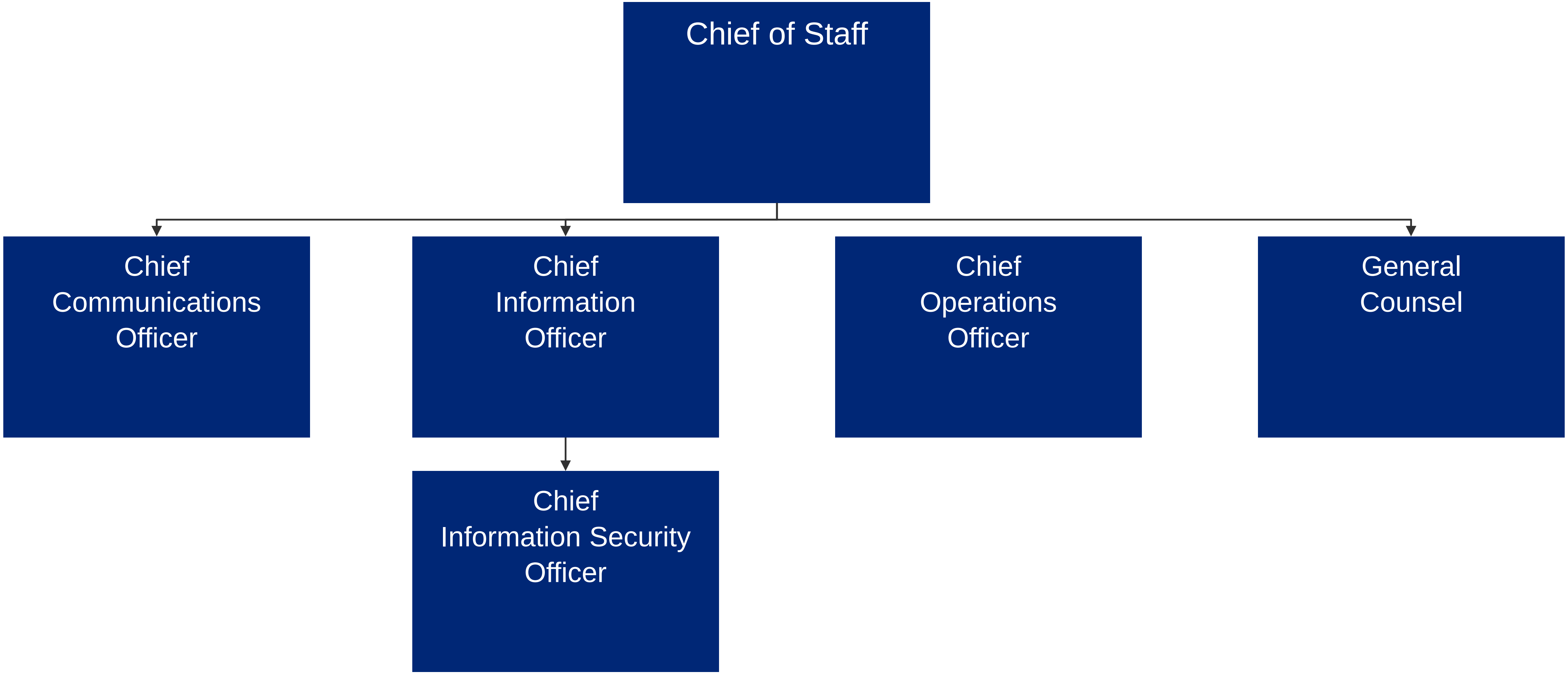
When taking action…

- Describe your thought process, including any assumptions, out loud
- Announce what the action is, who will do it, and how it will be done
- Determine if any approvals are necessary

To consult with others…

- Talk directly to other players in the room
- Inform the facilitator if you want to speak to a non-player

Player roles



Chief of Staff

Chief Communications Officer

Chief Information Officer

Chief Operations Officer

General Counsel

Chief Information Security Officer

Questions?

We are about to begin…

State governments are a target…

Citizen impact is a top concern

States collect, share and use large volumes of the most comprehensive citizen information.

Cyber incidents impact state business by affecting citizen services, revenue collections, or result in unplanned spending. In addition, the impact to citizen trust could have a significant consequence.

The large volume of information makes states an attractive target for both organized cyber criminals and hactivists.

Cybersecurity responses are most effective when coordinated at the Governor or business executive level

Finding from Deloitte-NASCIO Cybersecurity Study

Maturing role of the CISO

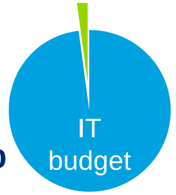
- CISO functions standardized; authority still an issue
- Communication still mostly ad hoc

39.6%
Governors

Budget-strategy disconnect

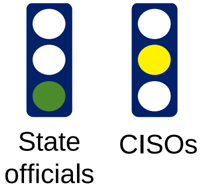
- Lack of funding is the top barrier
- States lag in spending as a percentage of technology

1-2%



Cyber Complexity Challenge

- Increasing threat sophistication
- Confidence gap



Talent Crisis

- Only 6 – 15 FTEs
- Talent scarcity

Barrier #3
59%

Source: Deloitte-NASCIO 2014 Cybersecurity Study

Manage what you can control

Secure.Vigilant.Resilient.™

Being
SECURE
means having risk-prioritized controls to defend critical assets against known and emerging threats.

Being
VIGILANT
means having threat intelligence and situational awareness to anticipate and identify harmful behavior.

Being
RESILIENT
means being prepared and having the ability to recover from, and minimize the impact of, cyber incidents.

Deloitte.