PARTNERS HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL

Anatomy of a Breach

Esmond Kane

Track 1-Core IT

9:45-10:30

Eden Vale Ballroom A

IS Tech Summit

May 19, 2016

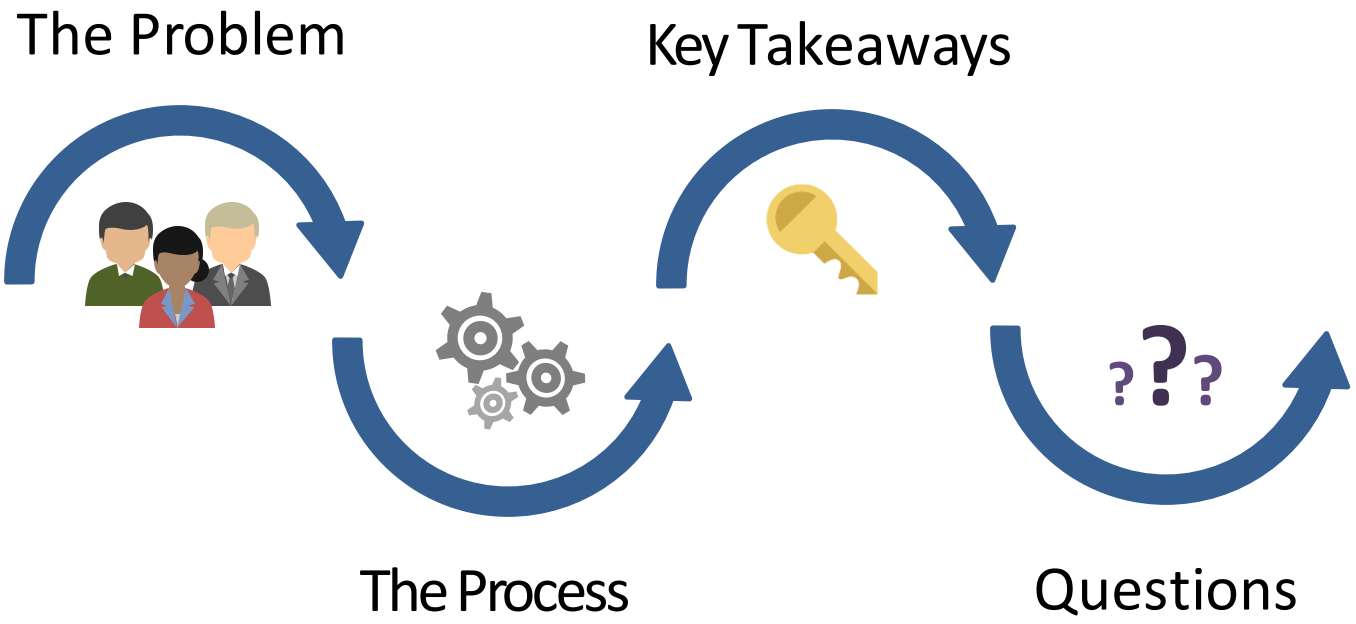
Anatomy of a Breach

IS Tech Summit

Esmond Kane

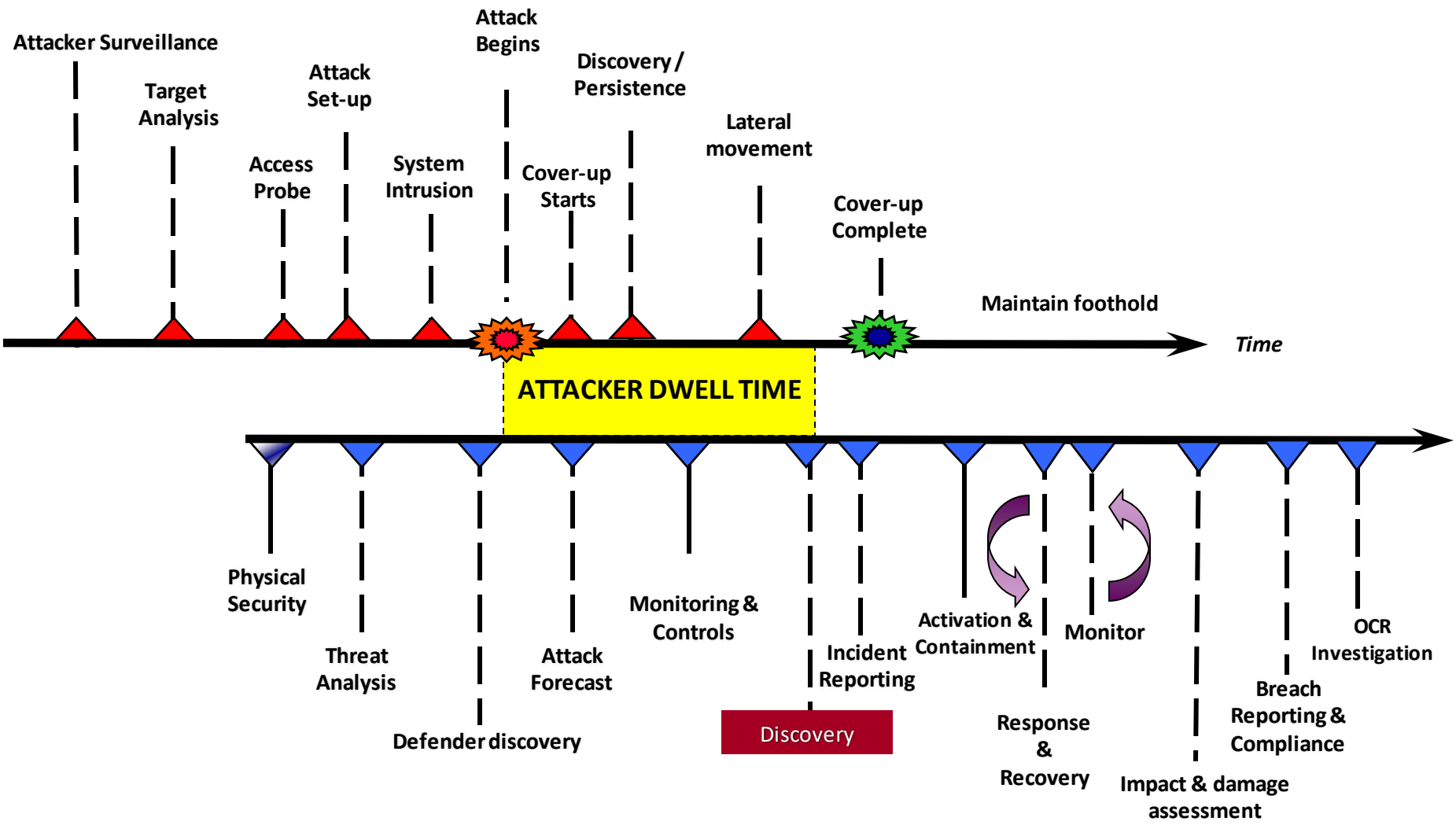
Esmond Kane is the Deputy Chief Information Security Officer in the Partners Healthcare Information Security and Privacy Office. In this role, Esmond is responsible for the operational component of the "Lighthouse" program, a radical transformation in Partners approach to security and privacy risk management. Prior to Partners, Esmond spent 10 years helping to guide improvements in IT delivery and information security in various roles in Harvard University. Prior to Harvard, Esmond spent 10 years in several roles and industries including KPMG and BIDMC.

Agenda



The Problem

Overview

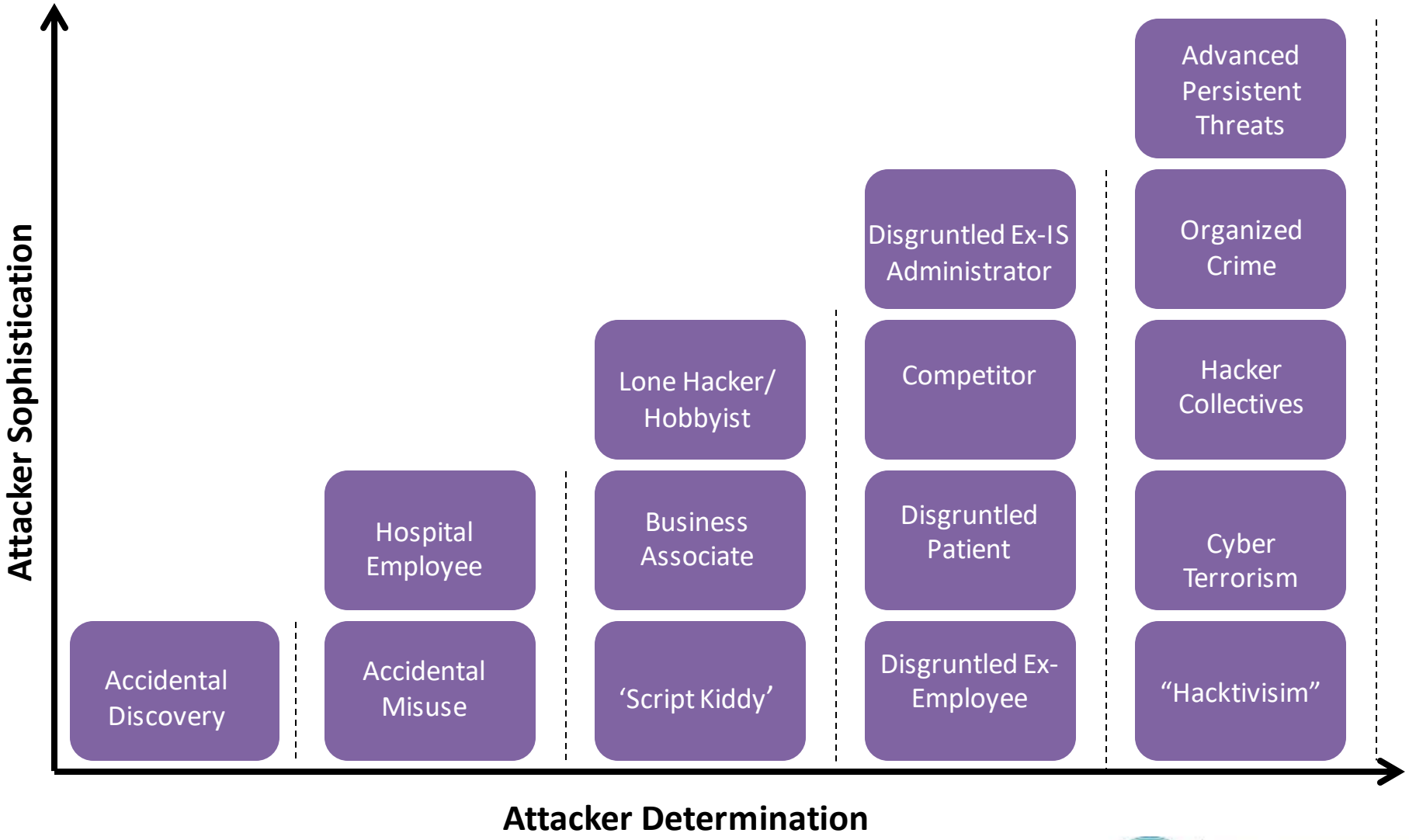


Source: Based upon NERC HILF Report (http://www.nerc.com/files/HILF.pdf)

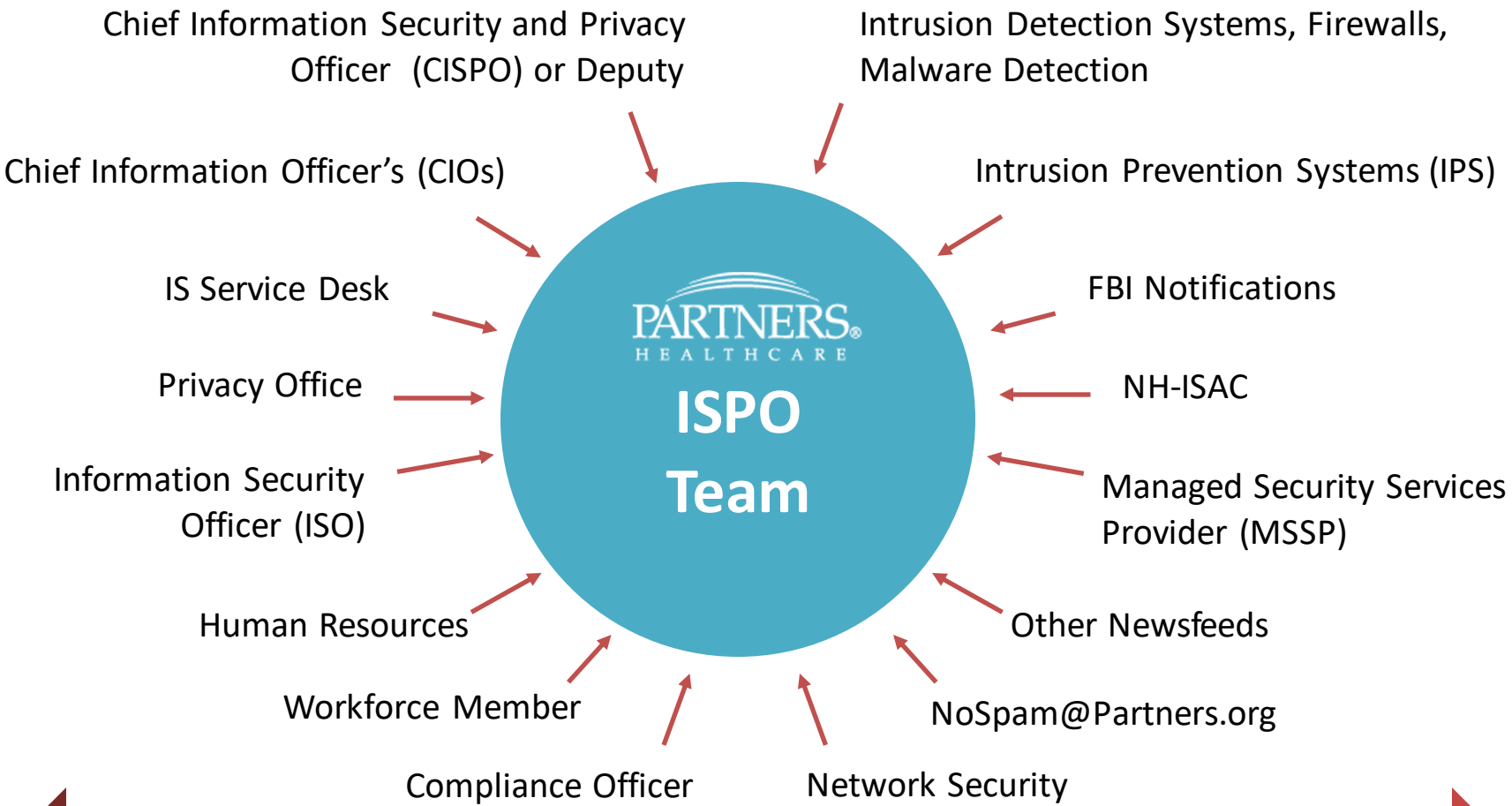
What is a Breach?

	Definition
Event	An event is an observable occurrence in a system or network.
Incident	An event reported to the designated privacy and/or security official that will result in an investigation to determine the possibility of an impermissible use or disclosure of PHI.
Breach	The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the CE or BA as applicable, demonstrates based on a risk assessment that there is a low probability that the PHI has been compromised.

Health Care Threat Actors



Intake Process



Partners Timeline

IS Tech Summit

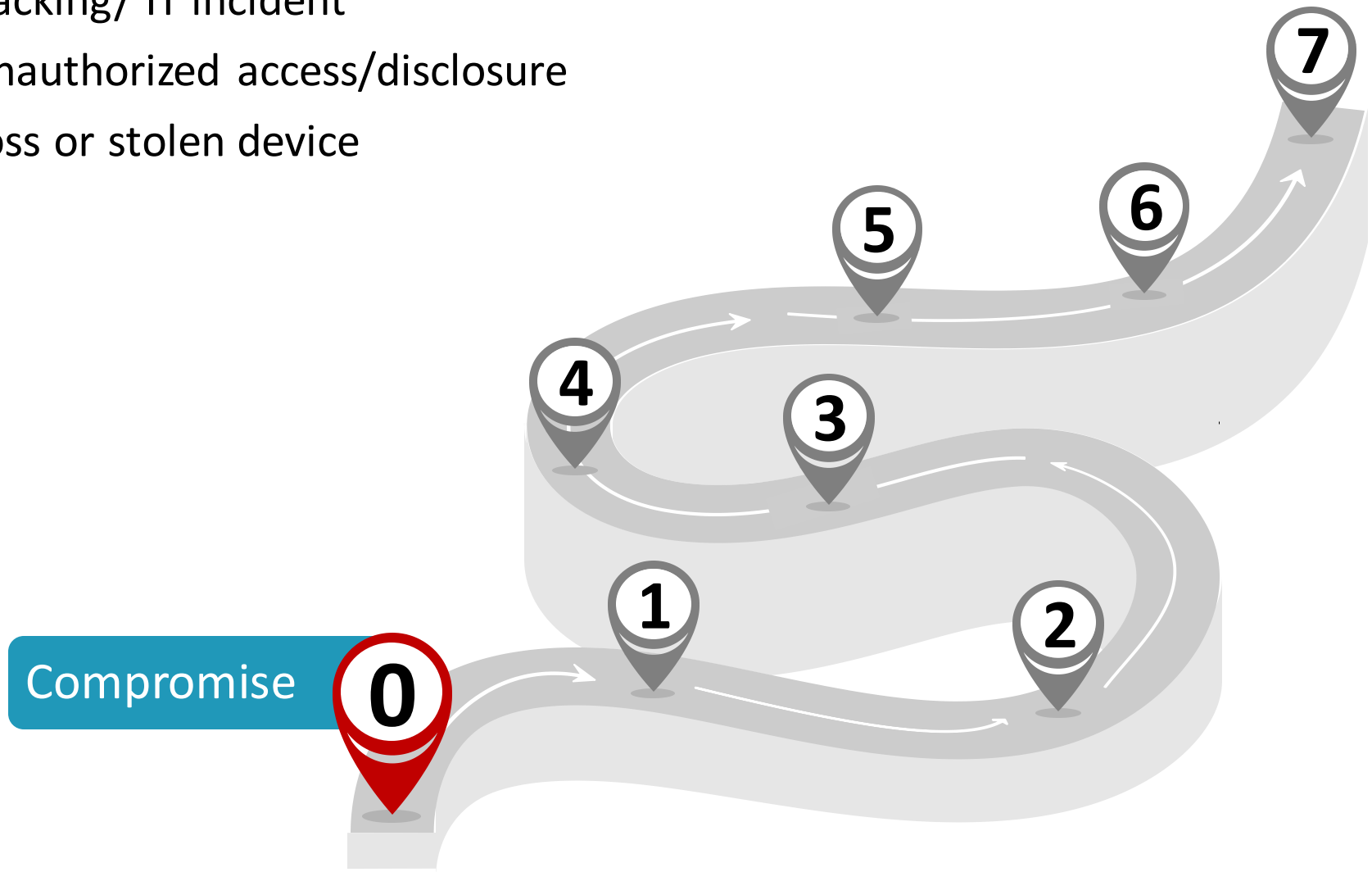
	Name of Covered Entity	Individuals Affected	Type of Breach	Location of Information
February 2015	Partners HealthCare System, Inc.	3,321	Hacking/ IT Incident	Network Server
July 2015	The McLean Hospital	12,694	Loss	Other Portable Electronic Device
July 2015	Massachusetts General Hospital	648	Unauthorized Access/Disclosure	Email
November 2016	Brigham and Women's Hospital	1,000	Unauthorized Access/Disclosure	Email

The Process

Compromise

IS Tech Summit

- Hacking/ IT incident
- Unauthorized access/disclosure
- Loss or stolen device



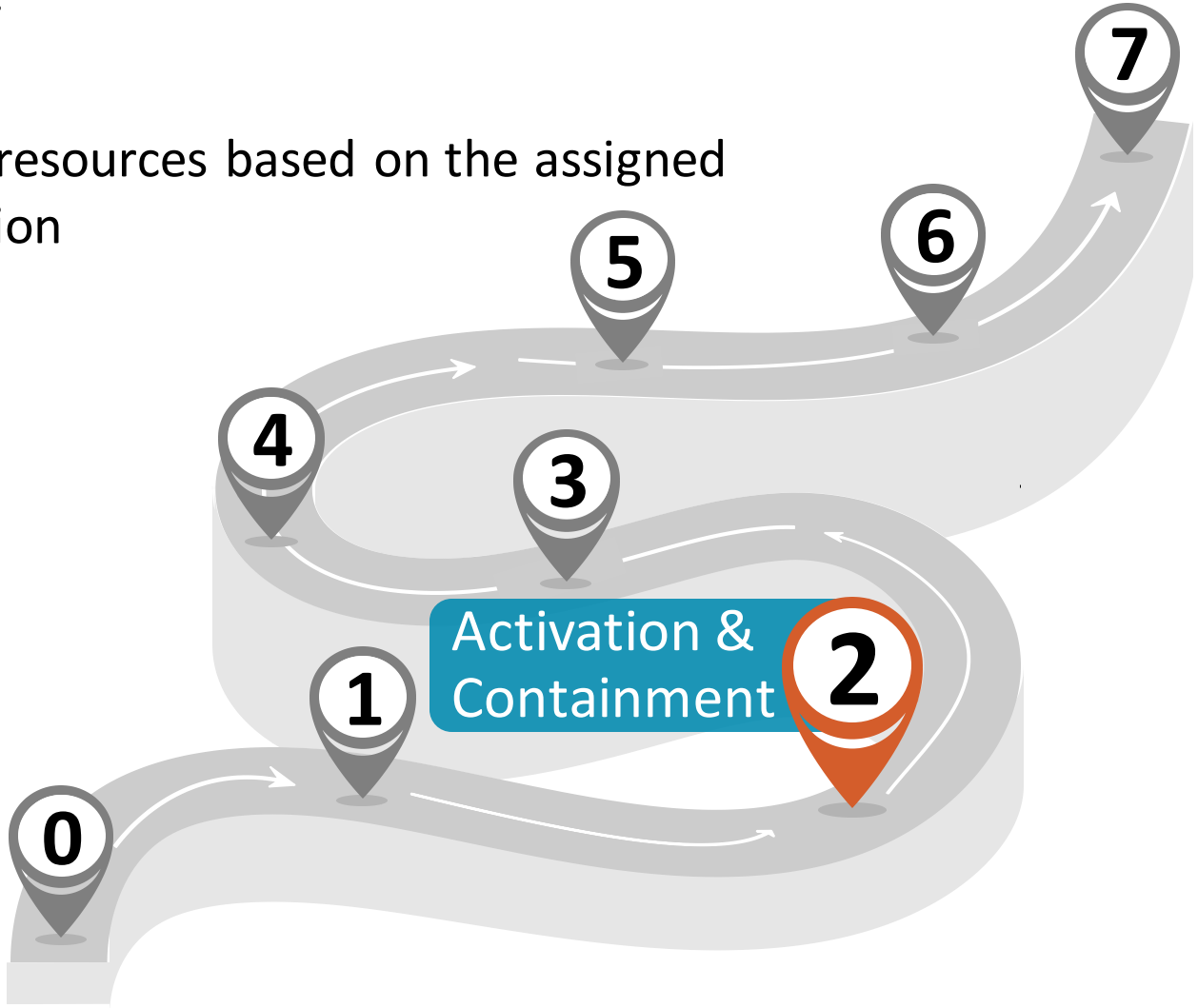
Discovery

- Confirmation of incident
- Determination of scope
- Categorization based on the actual or anticipated impact

Activation and Containment

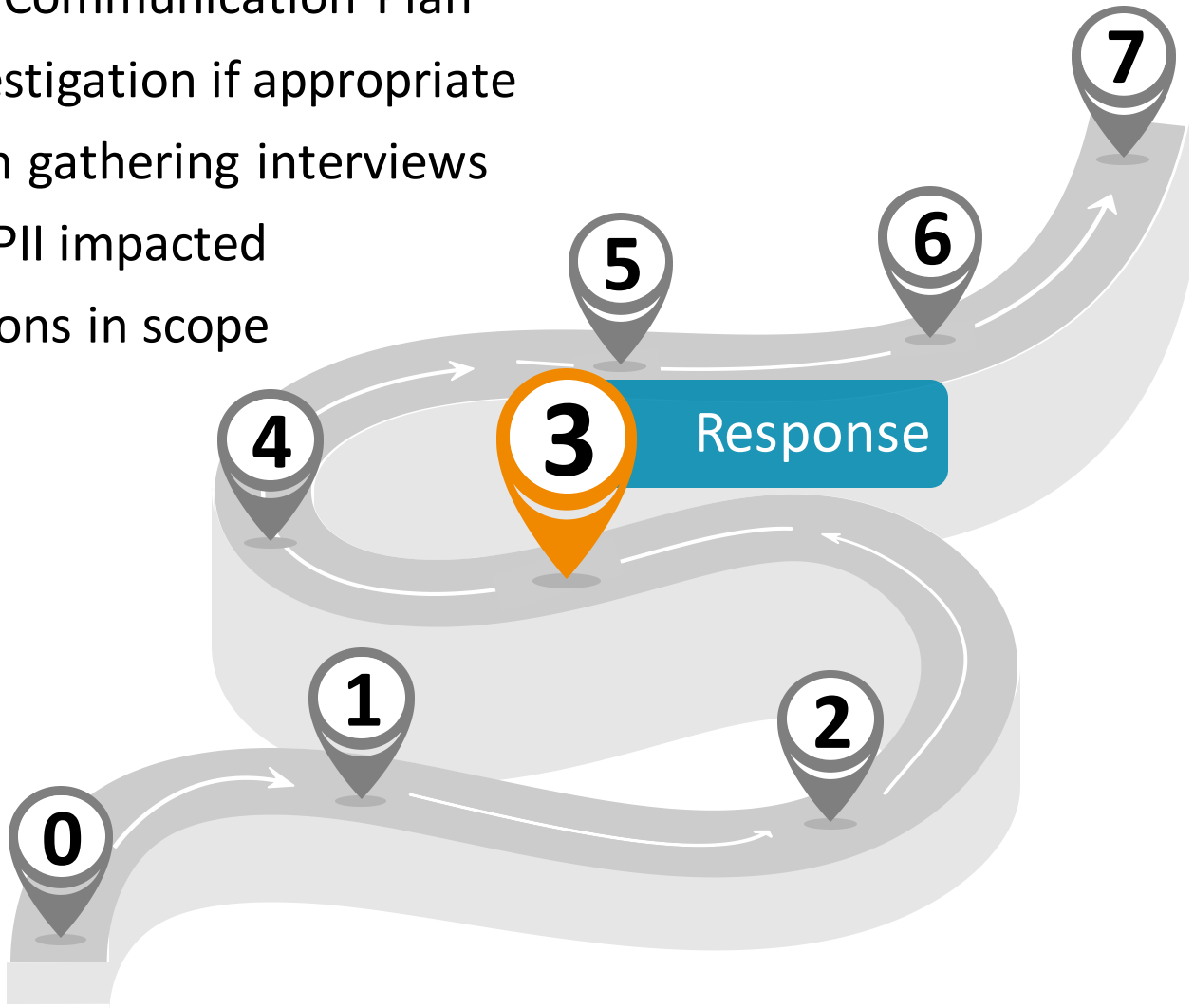
IS Tech Summit

- Contain the incident
- Preserve evidence
- Convene necessary resources based on the assigned incident categorization



Response

- Implement Incident Communication Plan
- Initiate forensic investigation if appropriate
- Conduct information gathering interviews
- Determine PHI and PII impacted
- Determine jurisdictions in scope



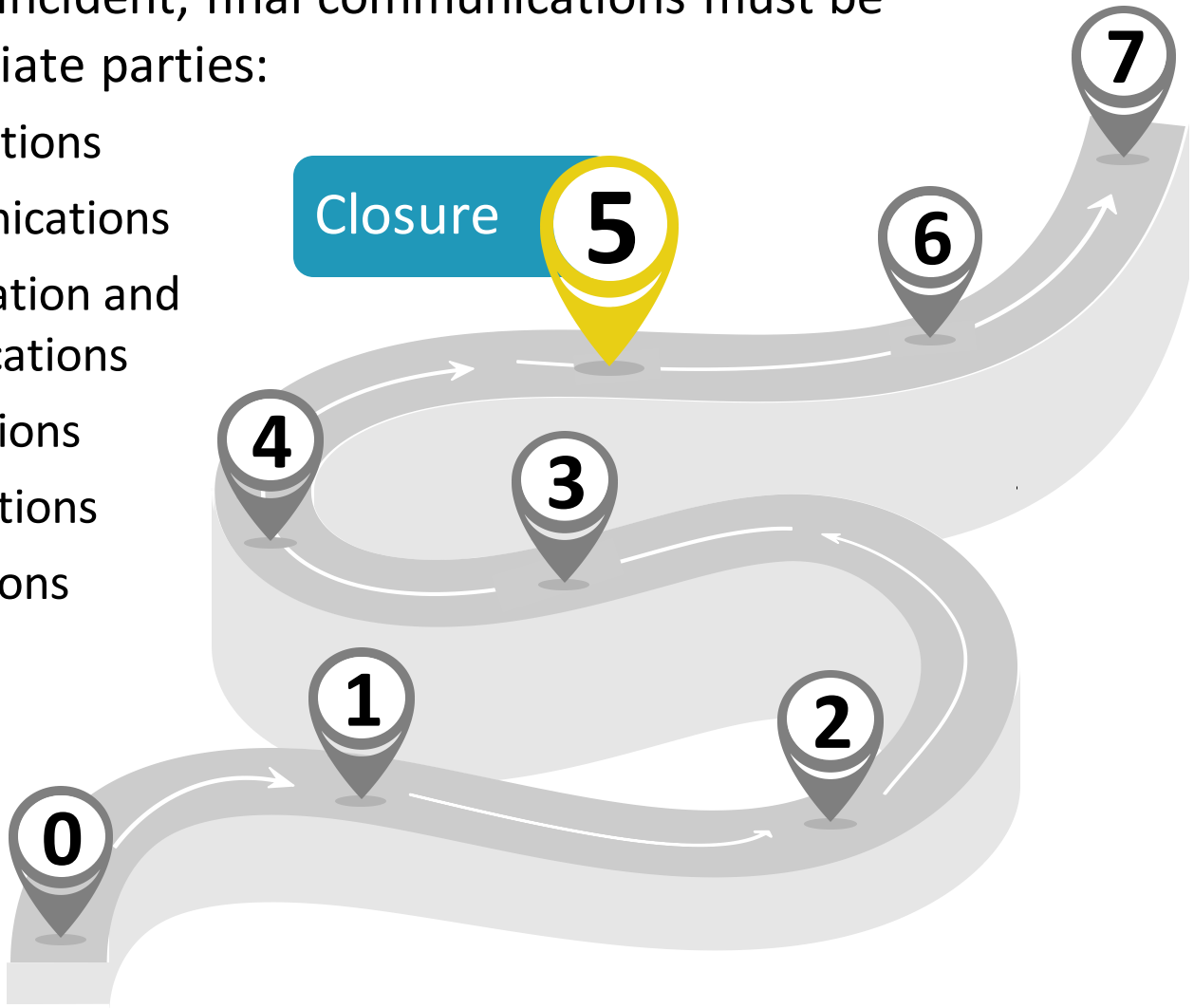
Monitoring & Recovery

IS Tech Summit

- Information Security Officer to continue to monitor and evaluate the situation

Closure

- In order to close an incident, final communications must be provided to appropriate parties:
  - Status Communications
  - Executive Communications
  - Response Coordination and Closure Communications
  - Legal Communications
  - Public Communications
  - Staff Communications



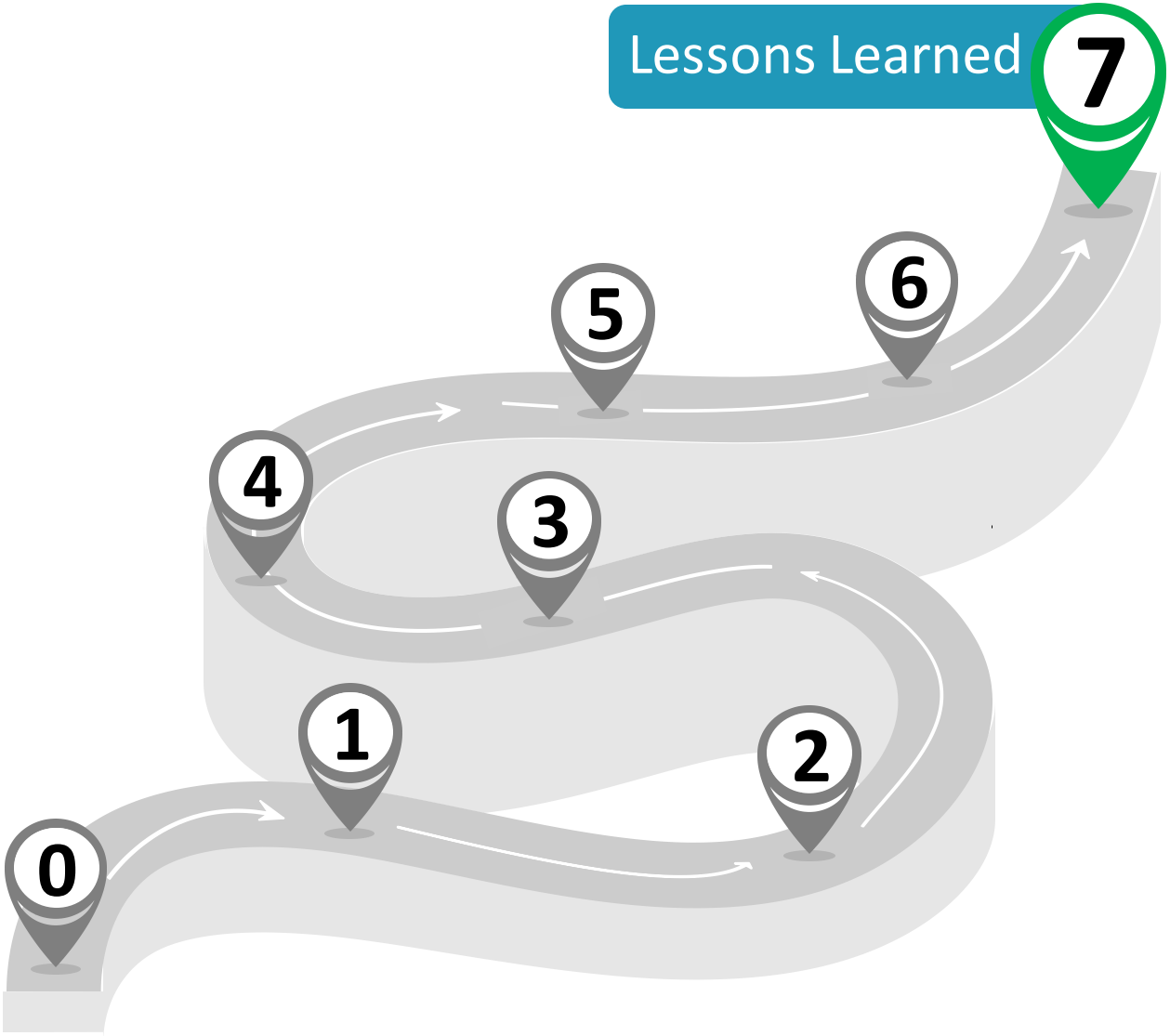
Investigation

IS Tech Summit

- OCR notification results in investigation
- OCR may issue Corrective Action Plan, if fined

Lessons Learned

- Debriefing session



Takeaways

Key Takeaways

- Be vigilant
  - Your caution and suspicion is invaluable
  - Your inattention can place us all in peril
- Be sensitive to time
  - We may only have 60 days to respond, sometimes less
  - Report issues ASAP to your ISO or Privacy Officer:
    - Security: http://intranet.partners.org/finance/hipaa/Security_3.asp
    - Privacy: http://intranet.partners.org/finance/hipaa/Privacy_3.asp
- Preserve evidence
  - Retain as much information as you can
  - Logs, logs and more logs
  - Think twice before a reboot
  - Maintain hardware, software and network inventory

What We All Can Do

- Be aware and educated
  - Think twice, click once
  - Limit social media and high-risk sites
  - Use strong passwords
  - Update and encrypt
- Talk with your teams. Be a champion

Questions

Esmond Kane
Information Security and Privacy
Email: ekane5@partners.org
Tel: (617) 726-9625