NCHICA Incident Response Workshop

Presented by:

Clyde Hewitt, CISSP, CHS, ISO 27001 Lead Auditor, Level III Program Manager

Executive Advisor, CynergisTek

CynergisTek was recognized in the 2016 KLAS Security Advisory Services report for having the highest overall client satisfaction, performance and impact on security preparedness in healthcare.

CynergisTek won the 2017 Best in KLAS award for Cyber Security Advisory Services.

Desired Learning Objectives

- Evaluate different non-technical incident vectors
- Apply knowledge to identify and respond to non-traditional incidents

INCIDENT RESPONSE POP QUIZ

Your Tasks

- Determine if if there is an incident
- Identify the key stakeholders who should be part of the incident response team
- Outline paths to perform a root cause analysis
- Is there a “Presumption of Breach”

Incident Management Exercise 1

- A business associate gets infected with ransomware, negatively impacting their operations for three weeks. The hospital was notified by the BA that no data was lost and the incident is not reportable, but no details are provided.

Incident Management Exercise 2

- One of the hospital employees who supports the billing process for an on-premises independent anesthesiologist practice loses a thumb drive containing the anesthesiology billing information.

Incident Management Exercise 3

- A printer supplier calls the head of procurement about maintenance payment delays. Apparently a newly hired buyer stopped authorizing payments because the printer supplier has not been submitting the Certificates of Destruction (CoD) with the invoices as specified in the contract. After a few calls, the head of procurement learns that the manufacturer does not have a chain of custody process, nor has ever submitted a CoD for failed warranty drives. This is something the previous buyer had neglected to notice.

Incident Management Exercise 4

- During the CFO's annual budget request meeting with the CEO, he/she asks why biomedical engineering submitted a 22% budget increase to replace a higher than anticipated number of medical devices on the "Could Not Locate" list.
- TASK: Who should be part of the Incident Response Team & WHY?

“It ain’t over until it’s over”

Post Incident Requirements

- 45 CFR §164.308(a)(6)(ii) *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes

Post Incident Requirements

- 164.414(b) (b) *Burden of proof.* In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402

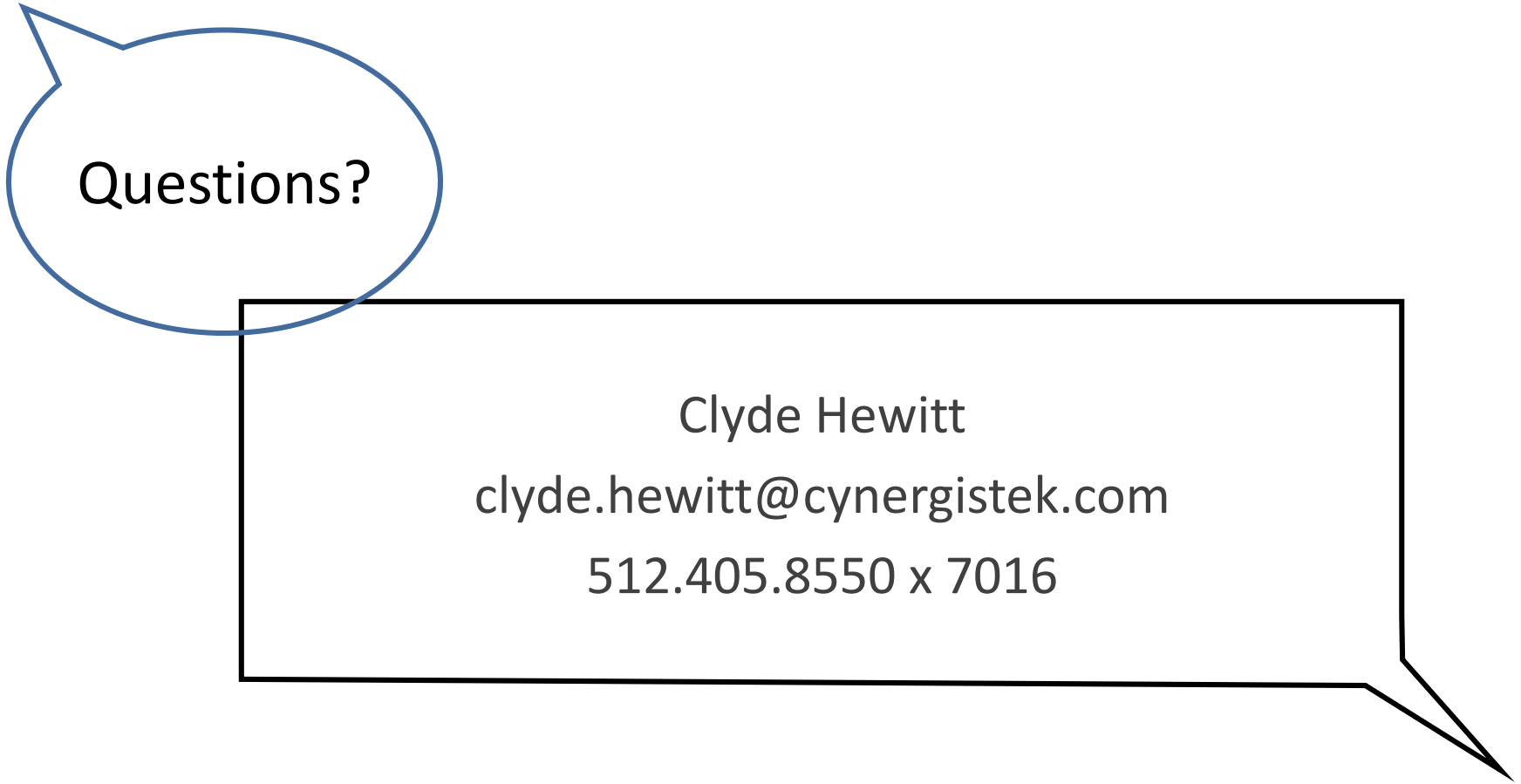
Presumption of a Breach

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Questions

Questions?


Questions?
Clyde Hewitt
clyde.hewitt@cynergistek.com
512.405.8550 x 7016