Demystifying the Mysterious World of Offensive Assessments

Presented by Lou Dignam and John R. Nye

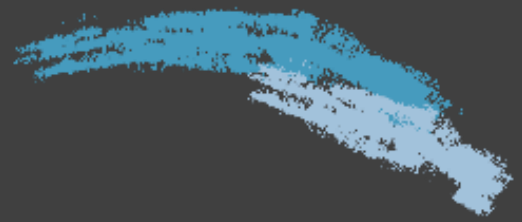
CynergisTek won the 2017 Best in KLAS Award for Cyber Security Advisory Services

CynergisTek has been recognized by KLAS in the 2016 and 2018 Cybersecurity report as a top performing firm in healthcare cybersecurity.

Agenda

1. Offensive Assessments
2. Advantages and Risks
3. How Maturity Should Guide
4. Real-World Impact
5. Talking to the Board
6. Conclusion

Offensive Assessments



What is an Offensive Assessment?

Dictionary

Enter a word, e.g. "pie"

of·fen·sive

adjective

1. causing someone to feel deeply hurt, upset, or angry.
   "the allegations made are deeply offensive to us"
   synonyms: insulting, insolent, derogatory, disrespectful, hurtful, wounding, abusive; More
2. actively aggressive; attacking.
   "offensive operations against the insurgents"
   synonyms: hostile, attacking, aggressive, invading, incursive, combative, belligerent, on the attack
   "an offensive air strike"

noun
/əˈfensiv/

1. an attacking military campaign.
   "an impending military offensive against the guerrillas"
   synonyms: attack, assault, onslaught, drive, invasion, push, thrust, charge, sortie, sally, foray, raid, incursion, offense, blitz, campaign
   "a military offensive"

Penetration Testing

- Often called a “pen test”
- An authorized attack
- External/internal/both
- Limited by scope
- Simulates malicious attack
- Same tools/techniques
- Finds holes before bad actors

Offensive Assessments – Phishing Exercises

- Tests user awareness
- Let’s people learn from mistakes w/o consequences
- Only proven method to reduce successful phishing
- Simulates varying levels of sophistication

Phishing is a Major Problem

- 91 Percent of Hacks Begin with an Email
  - According to a recent FireEye report based on 500 million emails sent between Jan. and June 2018
- Healthcare Lags Other Industries in Phishing Attack Resiliency Rate
  - This is the measure of the ration between those that report phishes and fall victim
  - Reported by PhishMe via HealthITSecurity.com

Offensive Assessments – Social Engineering

- Physical (on-site) SE
  - Tests physical security
  - Tests user awareness
  - Allows assessor/attacker to access physical systems
  - Assessor/attacker can use hardware hacks
  - Tests access to restricted areas
  - Shows vulnerability to physical theft

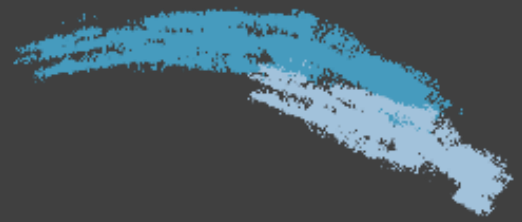
Remote Social Engineering
- Typically conducted via phone
- Tests user awareness
- Allows assessor/attacker to gather credentials

- Vishing
  - Do you know what this is?
  - It's more common than you think

Offensive Assessments – Red Teaming

- Brings it all together
  - Penetration testing of all in-scope systems
  - Often includes more in-depth testing as assessors are on-site
  - Phishing exercise can be used to gather credentials
  - Social engineering (physical) allows hardware and physical theft attacks gaining credentials

Advantages and Risks



Offensive Assessments Can Cause Offense

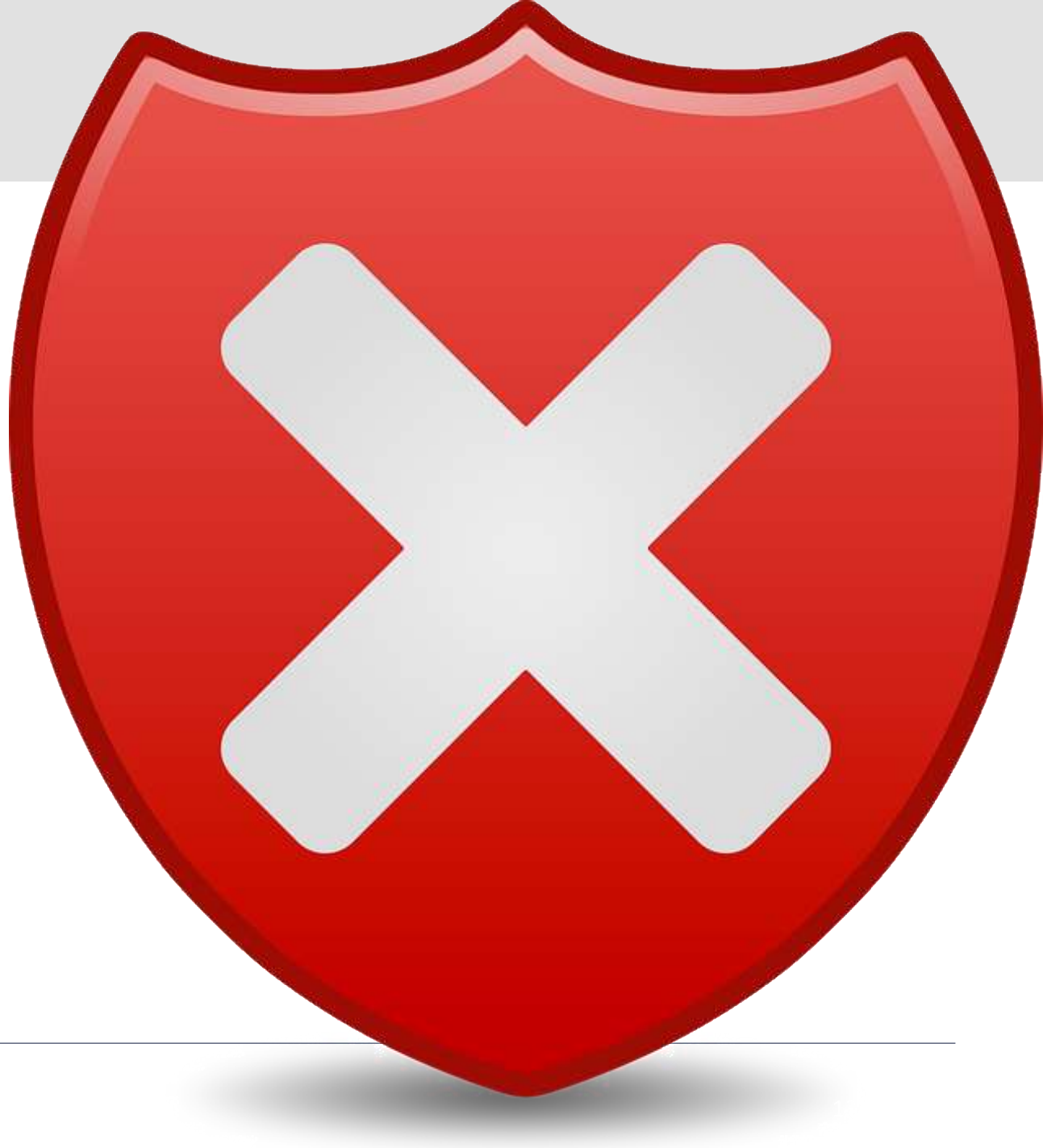
- Some systems can crash
- Sensitive information is accessed
- IT and security are often nervous and defensive
- Can cause downtime or outages
- Will show the flaws in your security and WILL make everyone nervous

Advantages Far Outweigh Risks

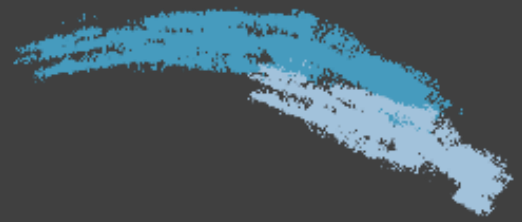
- Finding the holes before the bad actors do
- Eliminating vulnerabilities
- Finding unknown systems that present serious risks
- Minimize the chances of a breach
- Gain a broader understanding of your security posture

Biggest Selling Points of Offensive Assessments

- Most offensive assessments (which the exception of the Red Team) are a lot less expensive than you think.
- A good pentester will NOT crash your systems or cause outages.
- Offensive exercises show everyone in the organization how attacks look and how to be prepared.
- If you don’t do these the bad guys will gladly do it for you but the cost will be MUCH higher.

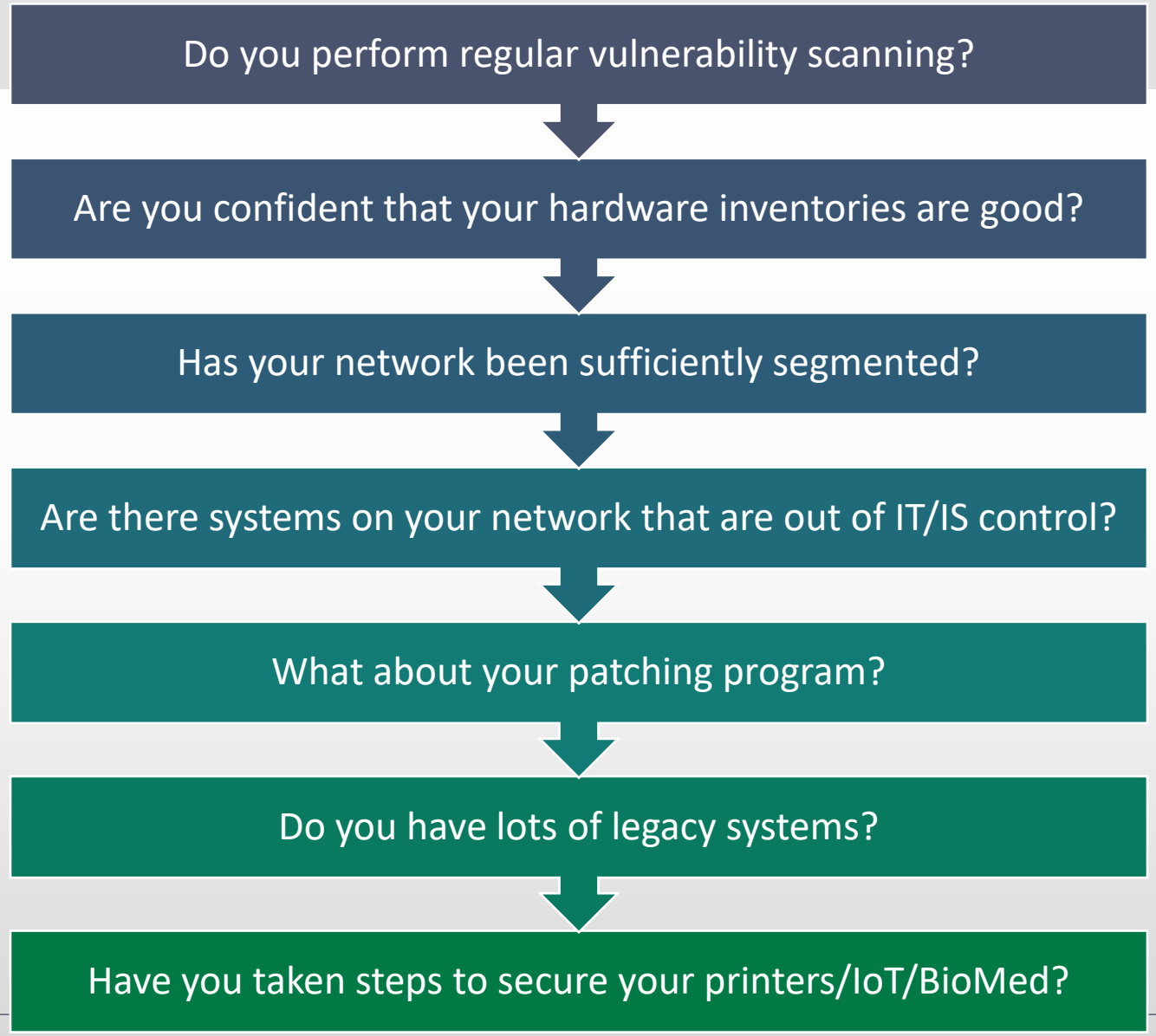


How Maturity Should Guide



Many Organizations Are NOT Ready

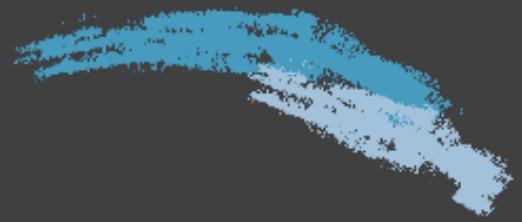
- Offensive assessments are proactive
- They find issues that are missed
- Can break systems that are not “ready”
- This type of assessment uses the “path of least resistance”
- Less secure/mature organizations will get less value



Is Your Organization Mature Enough?

Some Traits of a Mature Organization

Real-World Impact



Top Security Risks in Healthcare

Theft & Loss	Insider Abuse	Unintentional Action	Cyber Attacks
No change. Nearly half of all breaches involve some form of theft or loss of a device not properly protected.	Breaches in healthcare continue to be carried out by knowledgeable insiders for identity theft, tax fraud, and financial fraud.	Breaches caused by mistakes or unintentional actions such as improper mailings, errant emails, or facsimiles are still prevalent.	Majority of breaches reported in 2017 so far involved some form of hacking and represented nearly 99% of the records compromised.

Convergence = Opportunity

- In 2017, less than 1 in 10 providers had not adopted an EHR system, compared to the inverse in 2003
- Hacking has increase several hundred percent since 2015
- Ransomware attacks have soared to 80,000 per hour
- Breaches in 2017 are more about disruption and destruction than simple theft of data or extortion
- And the new concern is data corruption, the silent attacker

Breach Statistics (2015-2017)

58% of incidents involve insiders – healthcare has the highest percentage of incidents involving internal actors

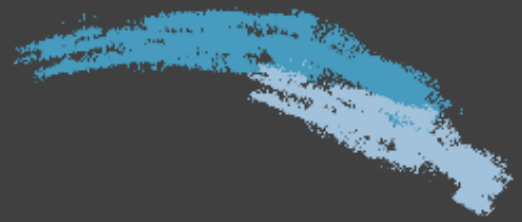
Medical device hacking creates media hype and presents greatest patient safety issue, but its still databases and documents most often involved

Ransomware is the top malware attack by a wide margin, 70% of attacks of malicious code were ransomware

Basic security measures are still not be implemented, data still not being encrypted, access not controlled

Verizon 2018 PHI Data Breach Investigations Report

Talking To The Board



The Board Needs to See Value

Security is abstract, the board needs to see a concrete value.

"Cybercrime damage costs will hit $6 trillion annually by 2021"

CSO Dec. 2016

Motive

"When there is an observable motive for a data breach, regardless of "whodunit," it's most often money. The access that healthcare workers have presents many opportunities for identity theft and fraud such as tax fraud, establishing lines of credit, etc."

-Verizon PHIBR 2018

Cyber Espionage: Intelligence

- Cyber espionage is being carried out by nation-state actors
- Large breaches such as Anthem, Premera, Community Health Systems, UCLA are suspected cases of espionage
- A case example is the OPM intrusion presumed by a Chinese group that captured security clearance documents
- But…they are also targeting industrial control systems that control and manage critical infrastructure

Targeted Attacks: Multiple Motivations

- Typically nation-state attack groups
  - "APTs are known for being highly sophisticated, using multiple vectors to attack a target network, and having unrelenting tenacity"
  - Many attacks go undetected for considerable periods of time – estimated 314 days on average
  - Phishing, ransomware, cryptomining have increased dramatically
  - Newer disruptive attacks replacing traditional data attacks

Are We Ready?

60% of IT security experts who responded to the Black Hat Attendee Survey believe that a successful attack on U.S. critical infrastructure will happen within two years. Also, only 26% of respondents believe that the country is prepared to handle such an attack.

Dark Reading, July 10, 2017

How Healthcare Stands Today – The Top Concerns

- **70%: lack of competent in-house staff**
- **67%: data breach**
- **59%: cyberattack**
- **54%: inability to reduce employee negligence**
- **48%: ransomware**

Source: Ponemon Institute Survey and Opus

- **84% of HCOs do not have a cybersecurity leader**
- **Only 15% of organizations have a CISO currently in charge**
- **Over 50% of all respondents said they do not conduct regular risk assessments**
- **92% of C-suite said data breach and cyber still not a key area of focus for the board**

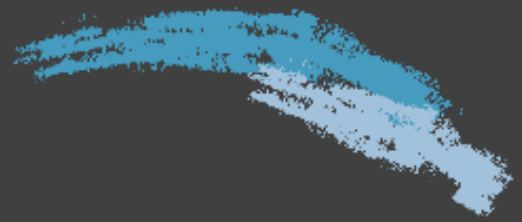
Q4 2017 Black Book survey (323 strategic decision makers in US HCOs – provider and payer

Priorities

- **89% of respondents said their 2018 budgets were dedicated to business functions**
- **“Only a small fraction” was being saved for cybersecurity**

Q4 2017 Black Book survey (323 strategic decision makers in US HCOs – provider and payer

Conclusion



Are We Ready?

Executives need to recognize that compliance does not equal security and checking the box is no longer sufficient.

Thank You!

John R. Nye
Sr. Director, Cybersecurity Research,
CynergisTek
john.nye@cynergistek.com
402.718.6631

Lou Dignam
CISO, Virtua
ldignam@virtua.org