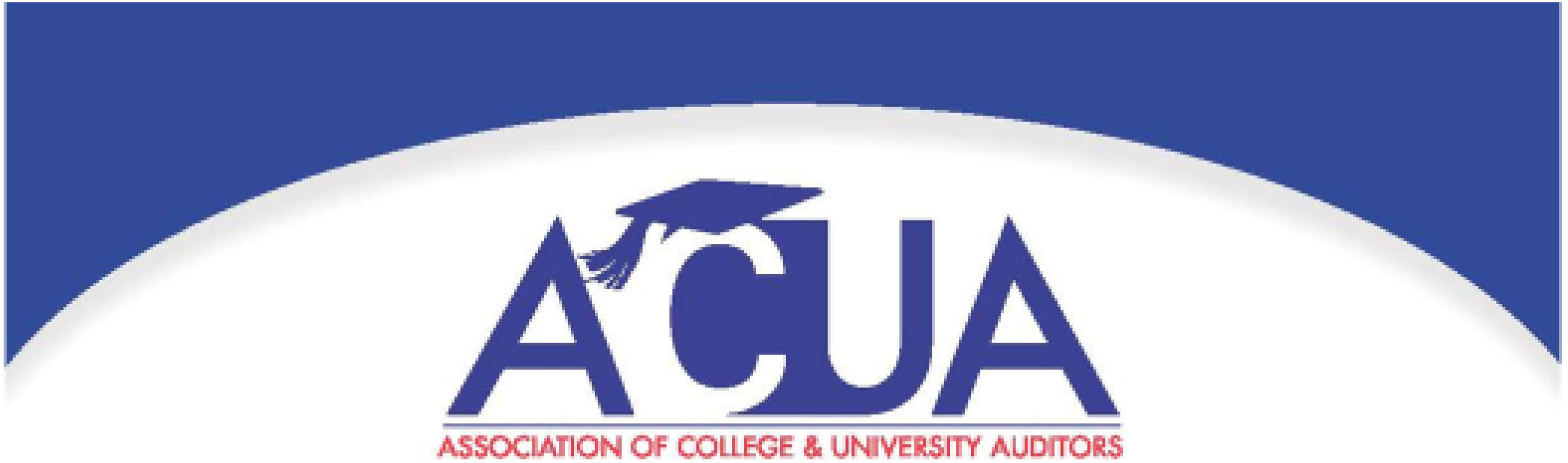


Did you know that Connect ACUA can send community discussions to your email in a real time, daily digest, or weekly digest format?

For more details, check out the Quick Tip post on

Connect.ACUA.org

Your Higher Education Auditing Connection

Penetration Testing – What Is It Good For?

Eric Randle

November 15, 2017

WEBINAR MODERATOR

- Don’t forget to connect with us on social media!

ACUA Distance Learning Director

Jana Clark

Senior Internal Auditor
Kansas State University

TODAY'S PRESENTER

Eric Randle, Senior Penetration Tester at Creative Breakthroughs, Inc.

Former IT Auditor, IT Asset Manager and Security administrator, and systems administration at the University of Michigan

(734) 926-5159

erandle@cbisecure.com

Agenda

- Introduction
- Problems We're Trying to Solve
- Overview of Penetration Testing
- Value Add
- When to Test
- Tools and Resources

Introduction

- Employment
  - Creative Breakthroughs Inc.
  - University of Michigan
- Education
  - Ferris State University – B.S. CIS, MBA
- Certifications
  - OSCP, GWAPT, C)PTE, GMON, CISA
- Awards
  - 2016 SANS Crystal City SEC542 CTF Winner
- Volunteer
  - Michigan Cyber Civilian Corps – MiC3

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Did you know that Connect ACUA can send community discussions to your email in a real time, daily digest, or weekly digest format?

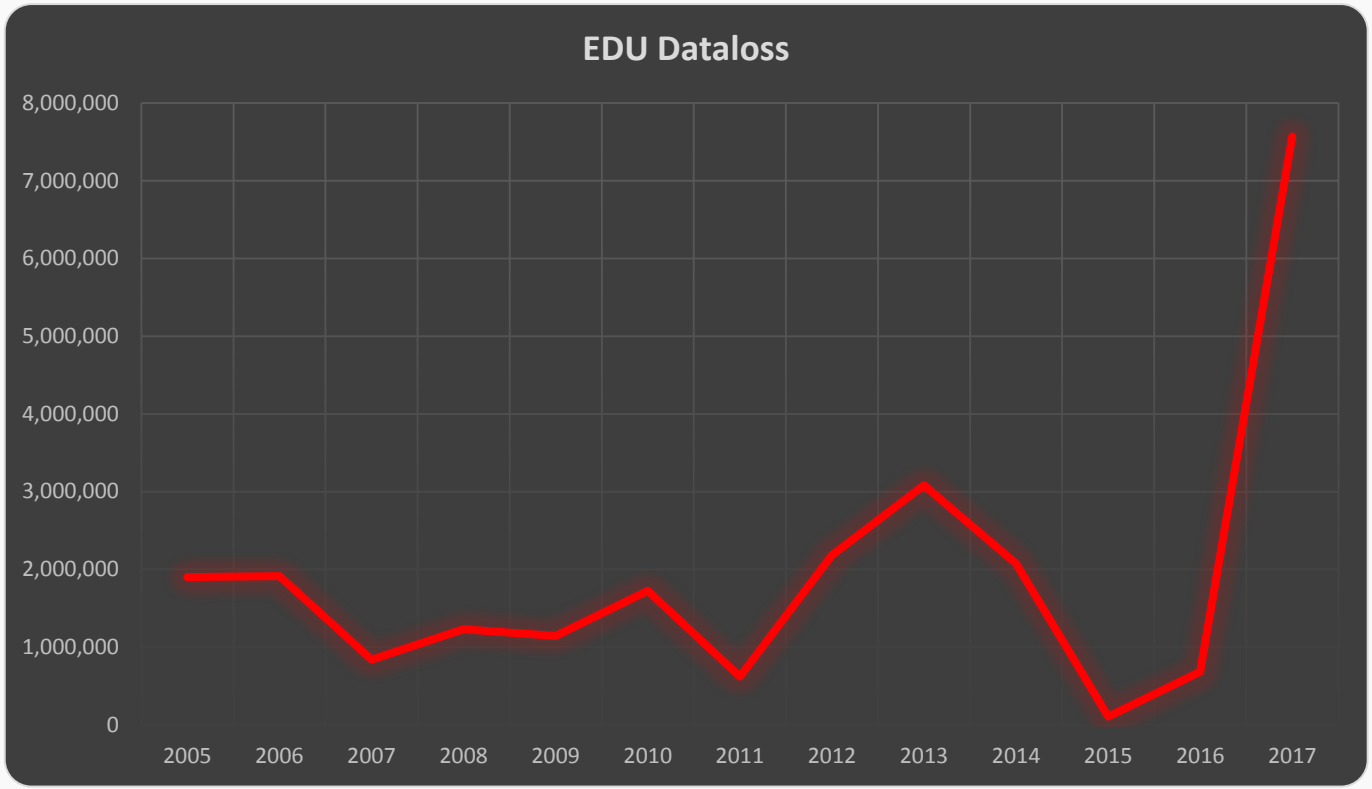
For more details, check out the Quick Tip post on

Connect.ACUA.org

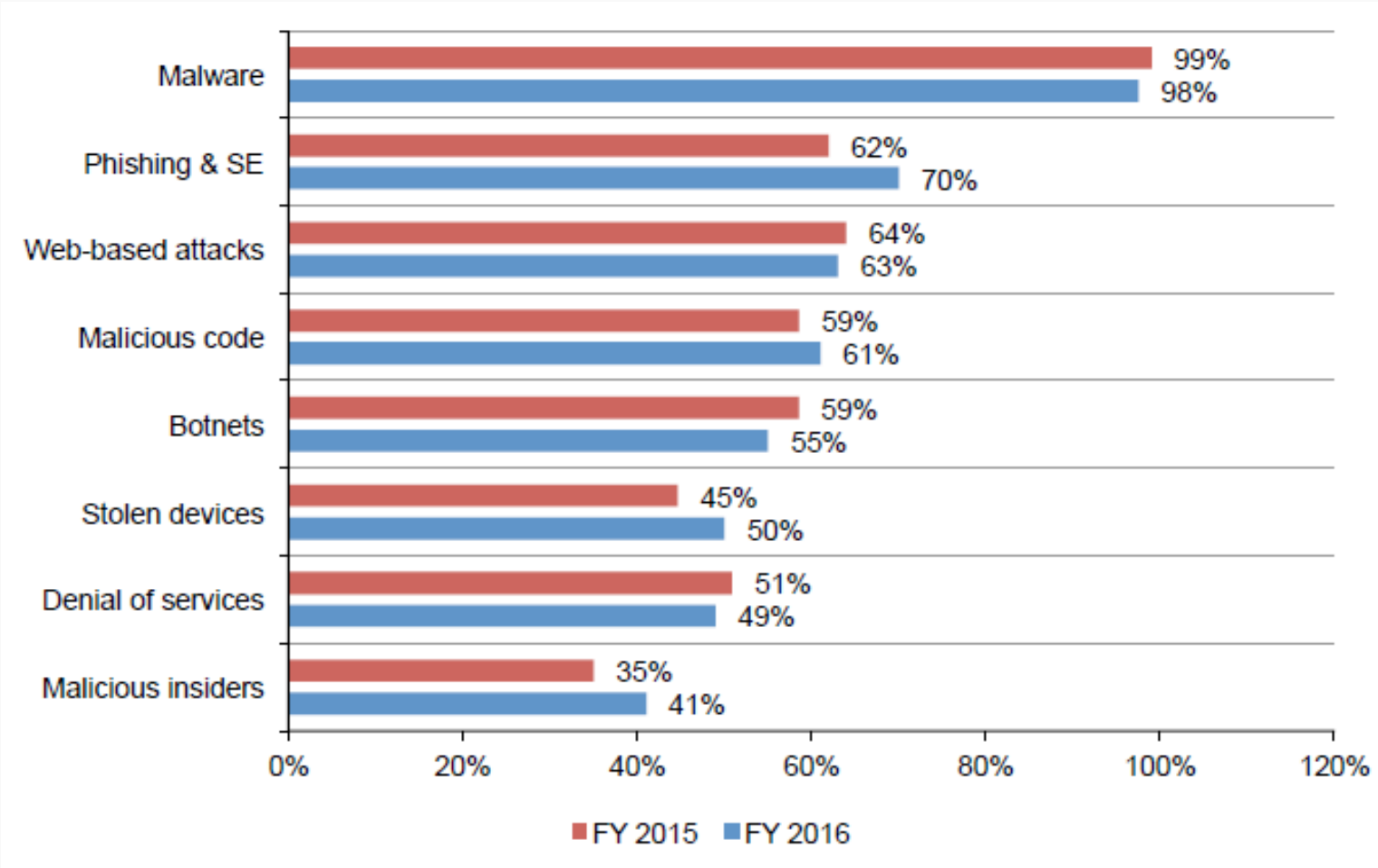
Your Higher Education Auditing Connection

Cyber Crime

- 798 Breaches Reported in EDU since 2005 (Likely More)
- > 25,000,000 Records Leaked
- Est. Cost $4,250,000,000

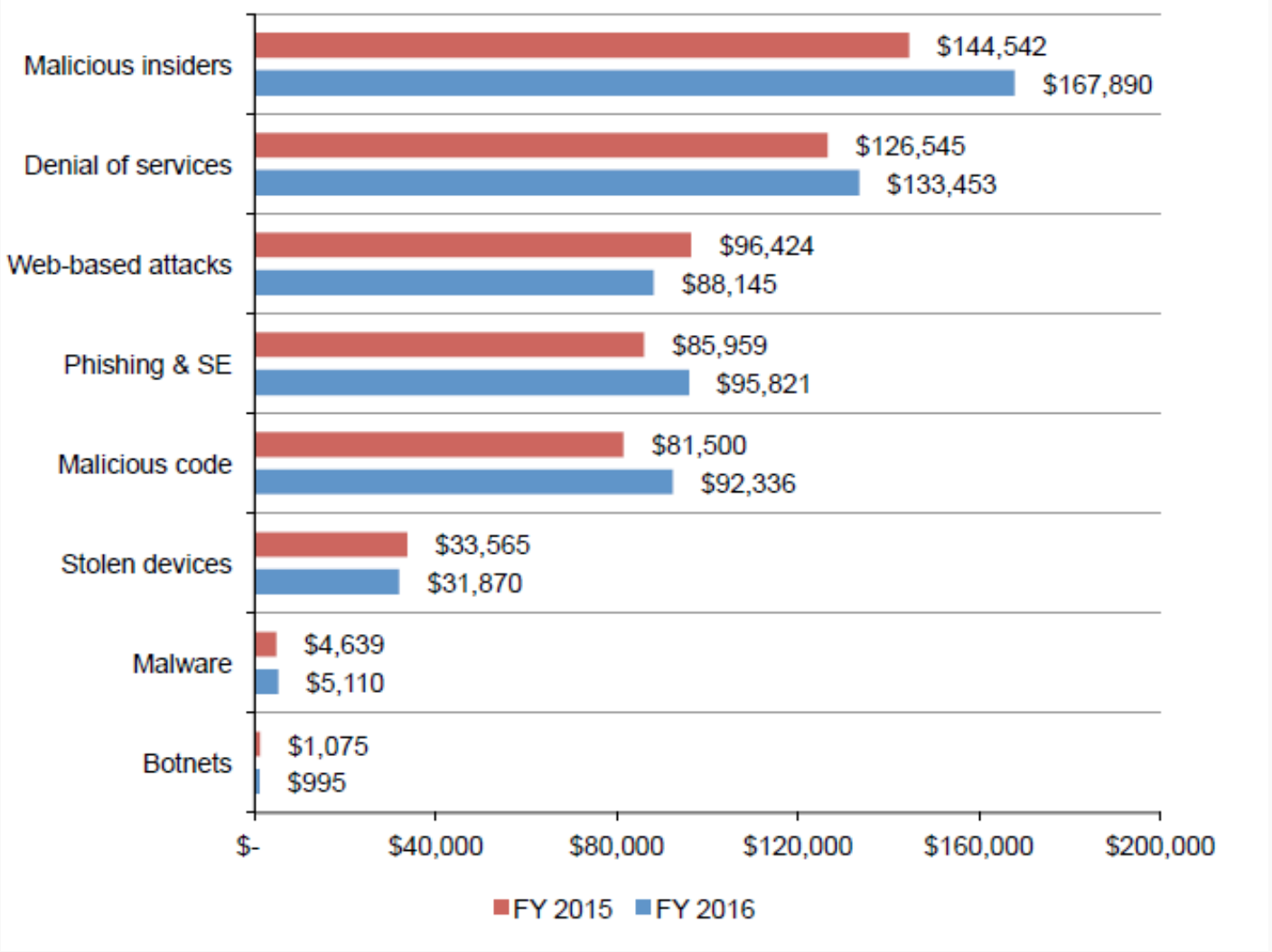


Types of Attacks



***237 Benchmarked Companies**

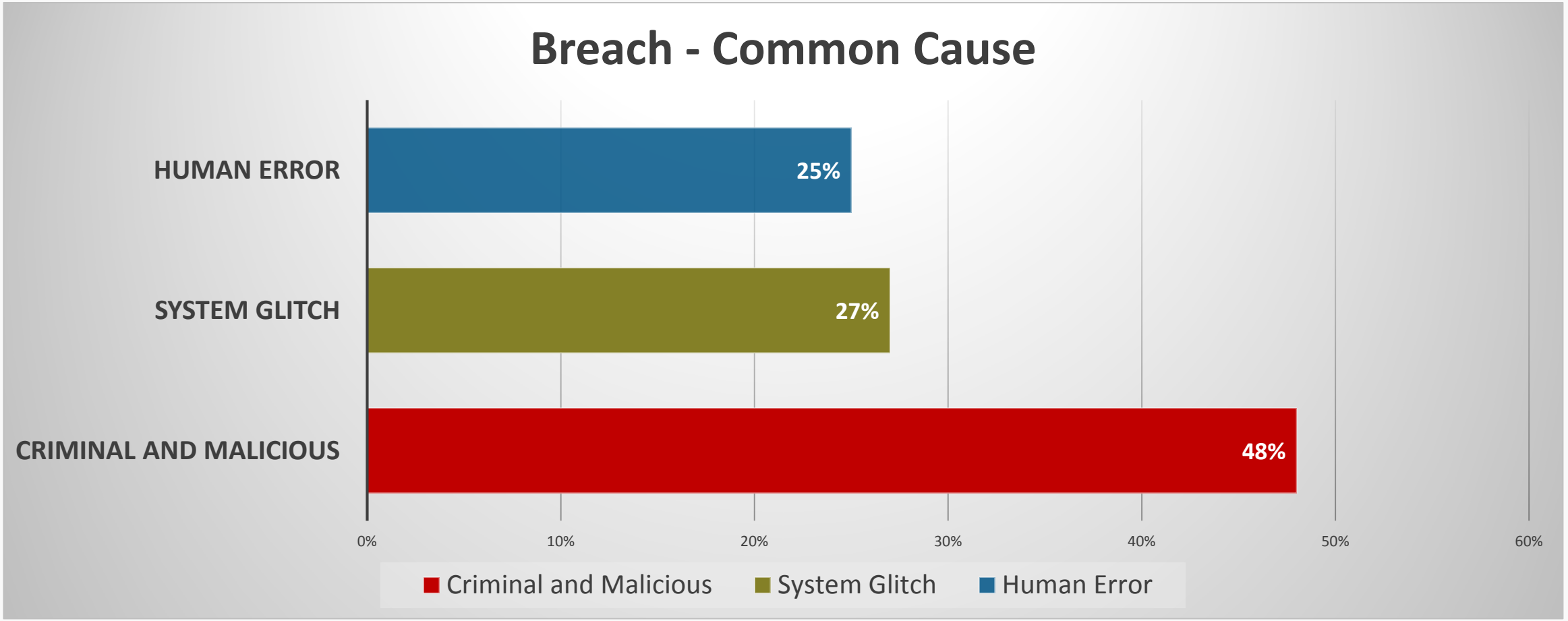
Cost of Attack Type



Polling Question #1

- Is cyber crime a driving factor in your audit planning?
  - Yes
  - No
  - Maybe

Source Of Breaches



Motivations

- Money
  - R&D Grants
  - Intellectual Property
  - Academic Research
- Hacktivism
- For Fun
- Theft of Resources
  - Amplification Attacks/DDoS
  - Library Subscriptions
- Spreading Chaos

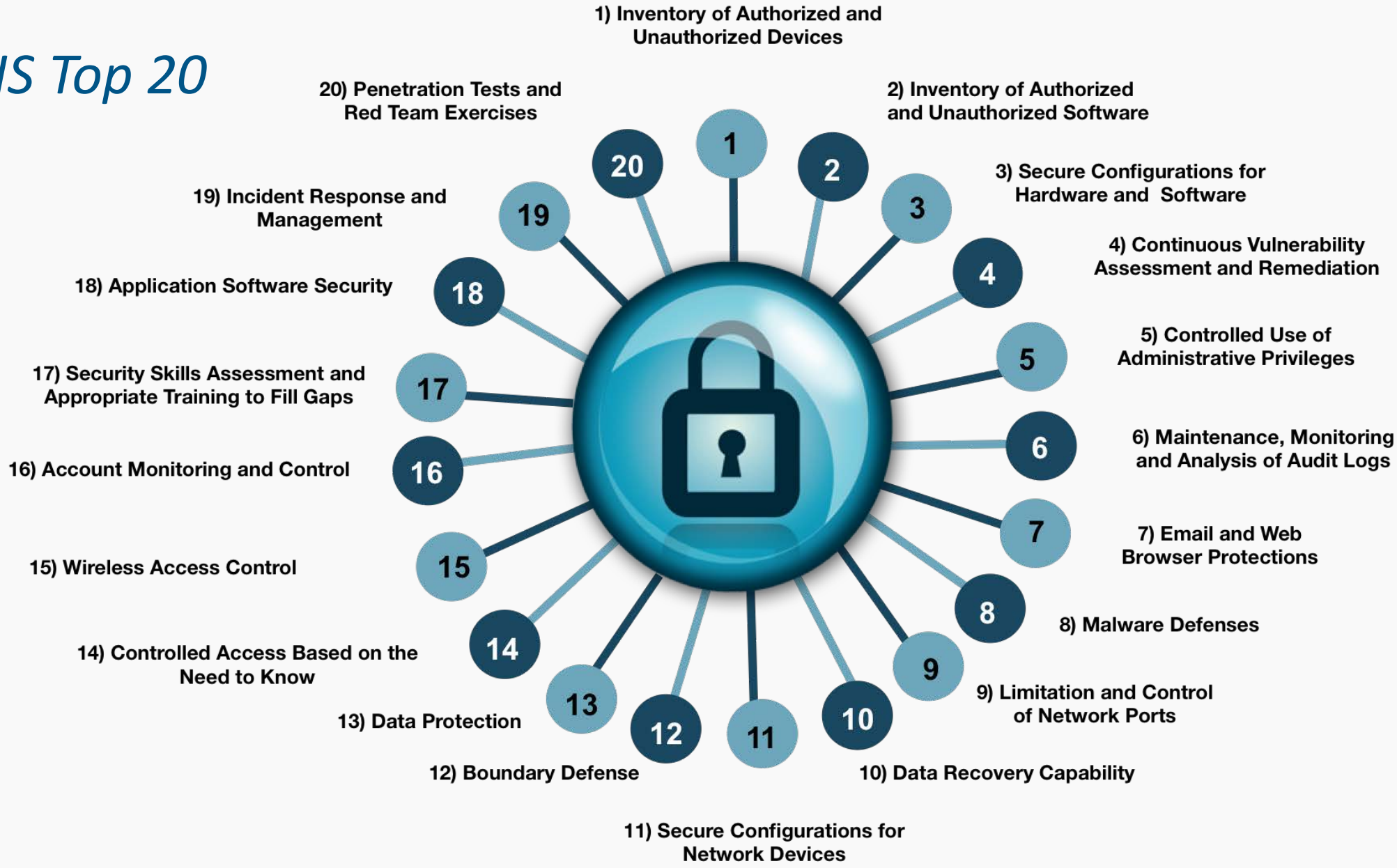
What Can Be Done?

- Culture of Information Security
  - People
  - Processes
  - Technology
- Leverage Best Practices
  - CIS Top 20
  - OWASP Top 10

Polling Question #2

- How would you rate your understanding of Information Security?
  - I’m an expert and regularly audit Information Security
  - I have an intermediate skill set but I am interested in learning more
  - I am a beginner that wants to perform information security audits
  - I’m just here for the CPE.

CIS Top 20


1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

OWASP Top 10

- Open Web Application Security Project
  - OWASP 2017 Top 10 RC2
    - A1 Injection
    - A2 Broken Authentication and Session Management
    - A3 Cross-Site Scripting (XSS)
    - A4 Broken Access Control
    - A5 Security Misconfiguration
    - A6 Sensitive Data Exposure
    - A7 Insufficient Attack Protection (NEW)
    - A8 Cross-Site Request Forgery (CSRF)
    - A9 Using Components with Known Vulnerabilities
    - A10 Under Protected APIs (NEW)

Penetration Testing

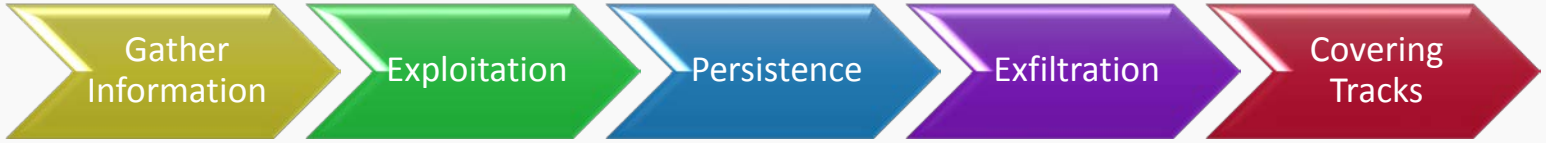
- Attacker Simulation
- Assessing Security Before Attackers Do
- Finding and Exploiting Security Weaknesses
- Looking for Ways an Attacker May Gain Access and Exfiltrate Data
- Testing User Education and Awareness
- Demonstrating and Communicating Risk

Let's Clarify

- Vulnerability Assessment
  - Finding all known vulnerabilities
  - Often automated
  - Performed Regularly
  - Measure Result Over Time
- Penetration Test
  - Exploitation of some vulnerabilities
  - Exploiting misconfigurations and control breakdowns
  - Hacking Humans
  - Vulnerability Scan Effective If Included

Attacker Methodology

- Information Gathering – OSINT
  - Passive Reconnaissance
  - Active Reconnaissance
- Exploitation
  - Password Spaying
  - Web Based Attacks
  - Phishing
- Exfiltration
  - Removing Data
- Gaining Persistence
- Covering Tracks



Penetration Testing Methodology

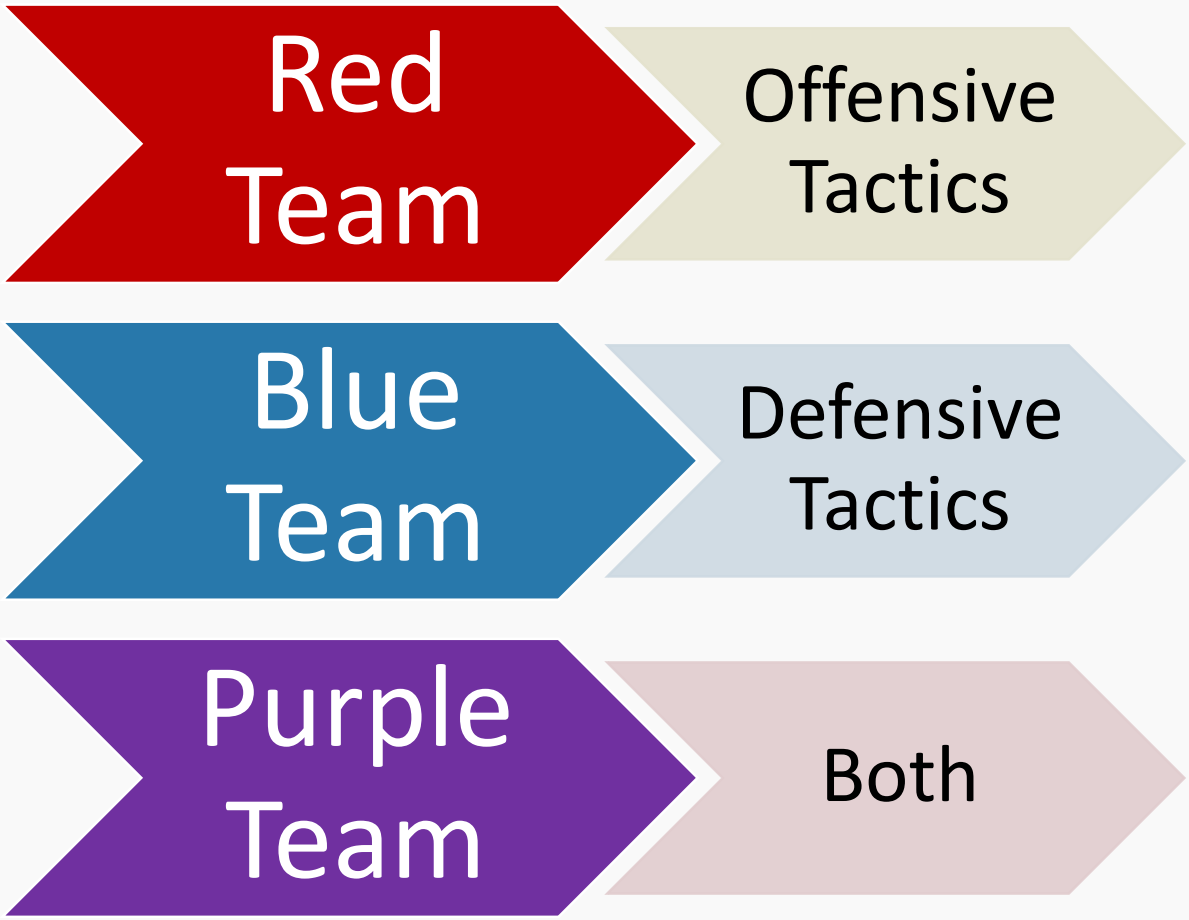
Polling Question #3

- Do you plan to acquire penetration testing services in the next 6 months?
  - Yes
  - No
  - Maybe

Penetration Testing Techniques

Black Box	• No knowledge of the environment in scope
Grey Box	• Some knowledge of the environment in scope
White Box	• Full knowledge of in-scope environment

Team Based Exercises



What Can Be Tested?

Networks

Applications

Web Applications

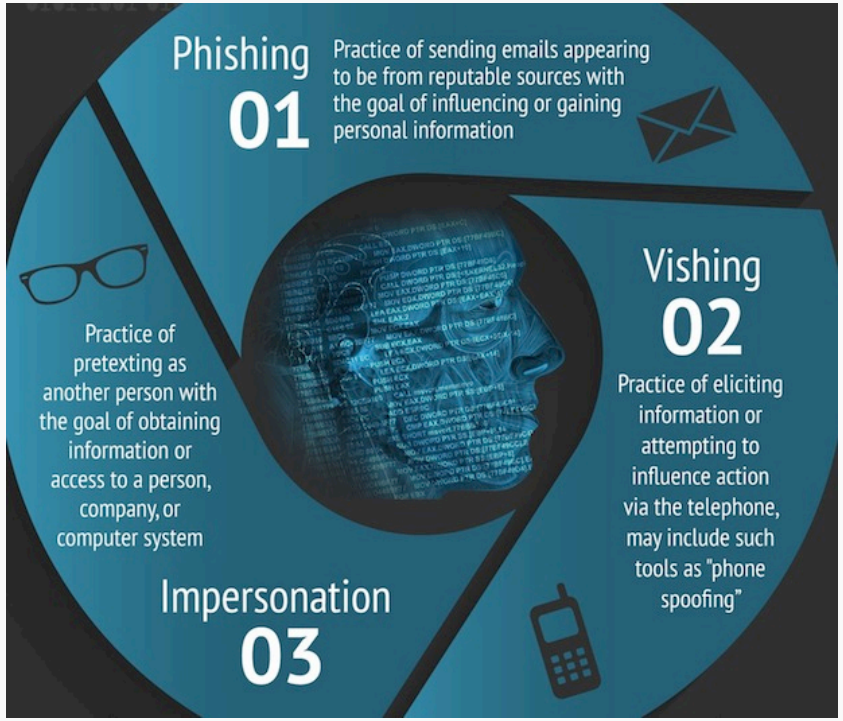
Mobile Applications

Physical Security

Humans – Social Engineering

Social Engineering

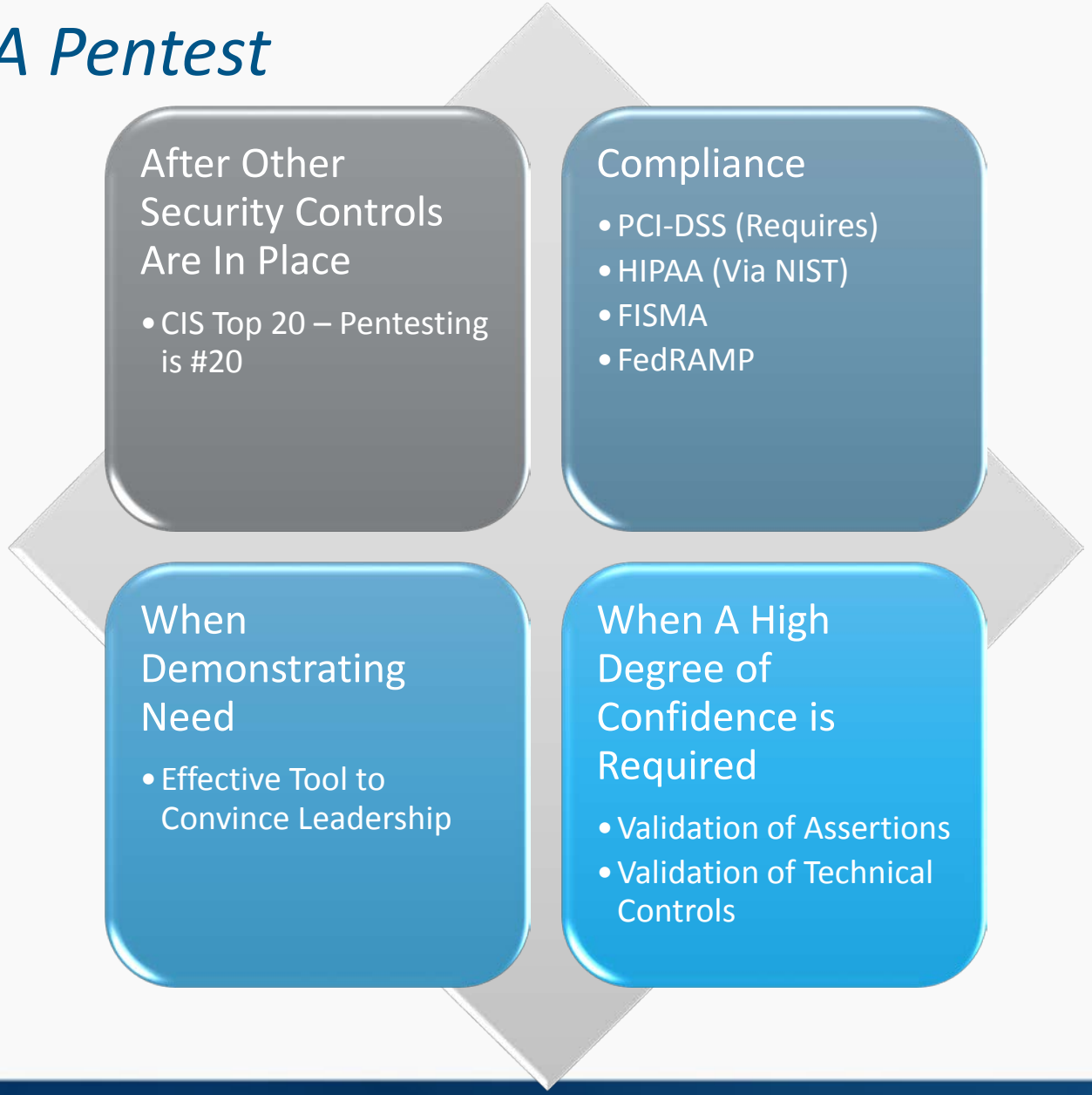
- Education and Awareness
  - Attackers Target Users
    - It's Effective
    - It's Easy
    - Hard to Detect
  - Regular Simulated Attack Exercises
    - Measure Over Time



Value

- Testing Security Controls
- Validating Technical Controls
- Validate Assertions
- Resource Prioritization

When To Do A Pentest



Tradecraft

Network Testing	• Nmap • Responder • Sparta
Wireless	• Aircrack-ng • Wifite • Hostapd-wpe
Web/Mobile Applications	• Burpsuite • OWASP ZAP • Commercial Products

Social Engineering

- Recon-ng
- KingPhisher
- Social Engineering Toolkit

Seeking Knowledge

Pre-Requisite

- Passion

Cybrary.it

- Penetration Testing and Ethical Hacking
- Advanced Penetration Testing

Offensive Security

- Penetration Testing With Kali

SANS

- SEC542: Web App Penetration Testing and Ethical Hacking
- SEC560: Network Penetration Testing and Ethical Hacking

Get Involved

- Local Communities
- Conferences

Polling Question #4

- Does your organization conduct penetration tests?
  - Yes
  - No
  - Not Sure

References

- https://www.privacyrights.org
- https://www.itchronicles.com/security/higher-education-big-target-cybercrime/
- https://securityintelligence.com/media/2016-cost-data-breach-study/
- http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Digital Citizens_CollegeInfoTheft.pdf
- https://www.owasp.org
- https://www.cisecurity.org/controls/
- https://Cybrary.it
- https://www.offensive-security.com/
- https://www.sans.org/

Thank You

- E-mail: erandle@cbisecure.com
- LinkedIn: https://www.linkedin.com/in/eric-randle-349ba65/
- Blog: https://kaizensecurity.wordpress.com/
- Twitter: @KaiZen_404

UPCOMING ACUA EVENTS

- November 30, 2017 – Managing Cybersecurity Assessments and Compliance (Baker Tilly)
- December 13, 2017 – Auditing Social Media (Felicia Best, TeamMate)
- December 19, 2017 – EU General Data Protection Regulations Impacting U.S. Institutions (Mark Bednarz and Ian Singer, PKF O'Connor Davies)
- February 7, 2018 – Construction Auditing (Asel Solovyeva (Univ of Michigan) and Robert Zellmer (Baker Tilly))
- March 18-21, 2018 – ACUA Mid-Year Conference in Louisville, KY