WHY EVERY AUDIT SHOULD BE AN INFORMATION SECURITY AUDIT

KIM Z. DALE, CISA, CISSP, FEDERAL RESERVE BANK OF CHICAGO

APRIL 9, 2018

AGENDA

Topic
Information Security and Why You Should Care
Types of Information Security Threats
Non-Technical Information Security Controls
Conclusion and Questions

OBJECTIVES

- By the end of this course, you will be able to:
  - Understand that information security is not just an IT issue
  - Recognize the information security impact of non-IT audit work
  - Learn how all auditors can help provide information security assurance in their organizations

WHO AM I?

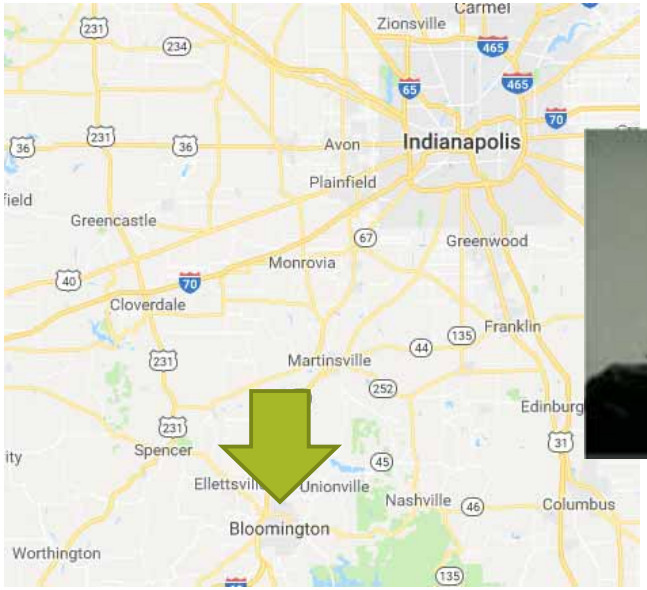
INFORMATION SECURITY IMPACTS EVERYONE

REASONS TO CONSIDER INFORMATION SECURITY IN YOUR AUDIT

1. Help your organization
2. Strengthen your other risk discussions
3. Help society

WHY I CARE ABOUT YOUR INFORMATION SECURITY

- Story time!



WHY I CARE ABOUT YOUR INFORMATION SECURITY

- Story time!

NOT ALL THIS WILL BE NEW

If you audit for fraud, you audit information security

WHAT IS INFORMATION SECURITY?

← Protect

Prevent →

TOUGH LOVE

Security and Usability Are Opposites

WHAT INFORMATION MIGHT NEED TO BE PROTECTED?

Digital Information

- Databases
- Documents
- Spreadsheets
- Emails
- Websites
- Presentations

Non-Digital Information

- Papers
- Trash
- Whiteboards
- What people say
- What people know

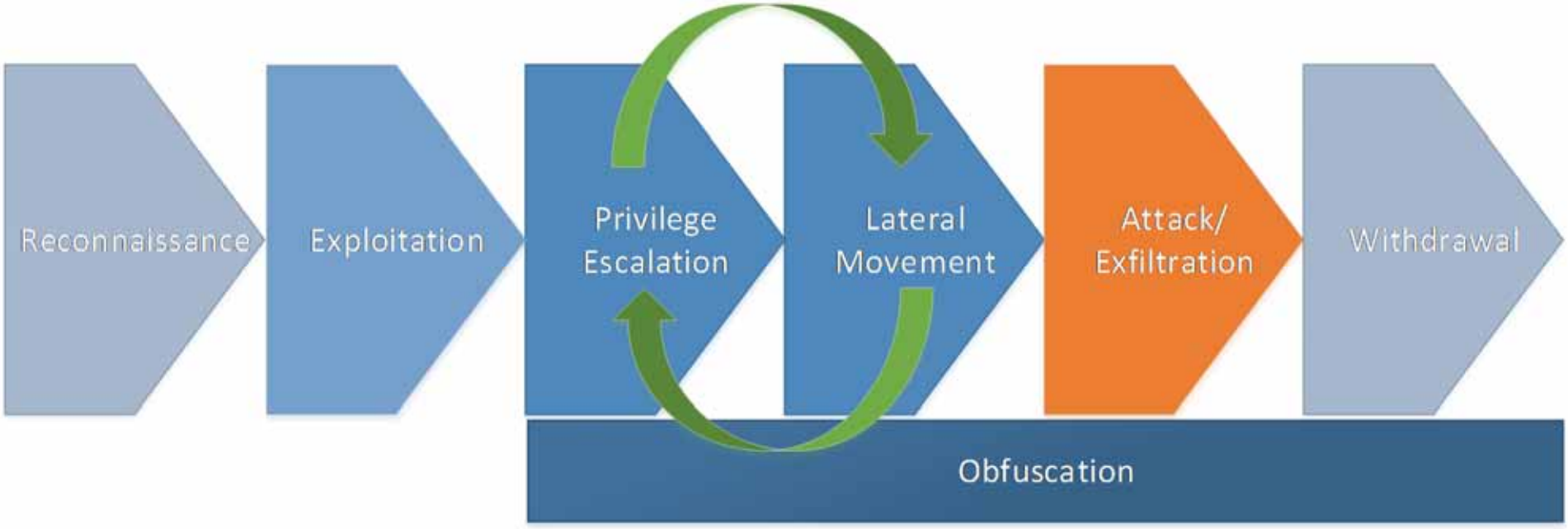
WHAT ARE THE THREATS TO INFORMATION SECURITY?

- Technical
- Non-Technical

INFORMATION SECURITY THREATS

(Obligatory Hacker in a Hoodie Stock Image)

ADVANCED PERSISTENT THREAT (APT)



PROBABLY YOUR LEAST FAVORITE SLIDE

- Audience participation time!

SOCIAL ENGINEERING

SOCIAL ENGINEERING

- The 2017 Verizon Data Breach Investigations Report (DBIR) reported
  - 43% of breaches included a social tactic

SOCIAL ENGINEERING

- Phishing
- Spear Phishing/Whaling
- Pretexting
  - Phone
  - On Site
- Websites
- USB Drives
- Bribery/Blackmail

INSIDER THREAT

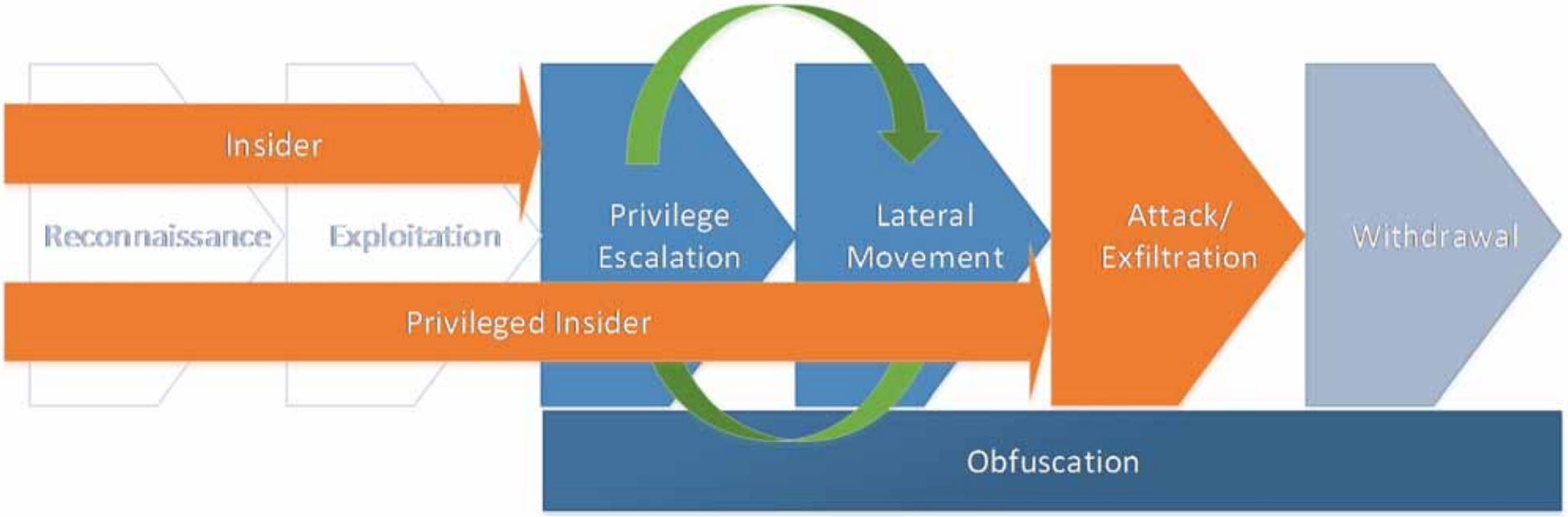
WHO IS AN INSIDER?

- A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data
- Source: Carnegie Mellon University Software Engineering Institute, CERT Division, Common Sense Guide to Mitigating Insider Threats, Fifth Edition

INSIDER THREAT

- The 2017 Verizon Data Breach Investigations Report (DBIR) reported
  - 25% of breaches involved internal actors

INSIDER ATTACK MODEL



TYPES OF INSIDER THREATS

	Malicious	Non-Malicious	
	Intentional		Unintentional
Accidental Leak			x
Espionage	x		
Financial Fraud	x		
Misuse	x	x	x
Data Theft	x	x	
Physical Theft	x		
Sabotage	x		
Violence	x		

LET'S TALK ABOUT CONTROLS

THE BEST CONTROLS LIMIT THE THREAT LANDSCAPE

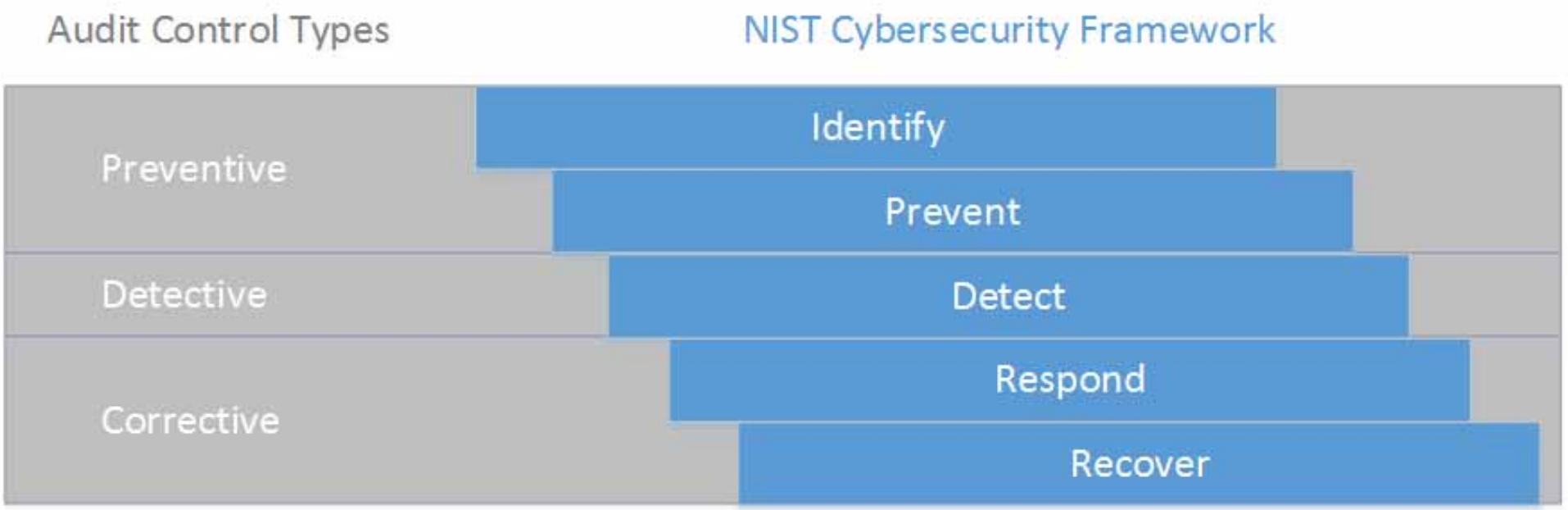
Information = Risk

Access = Risk

Connections = Risk

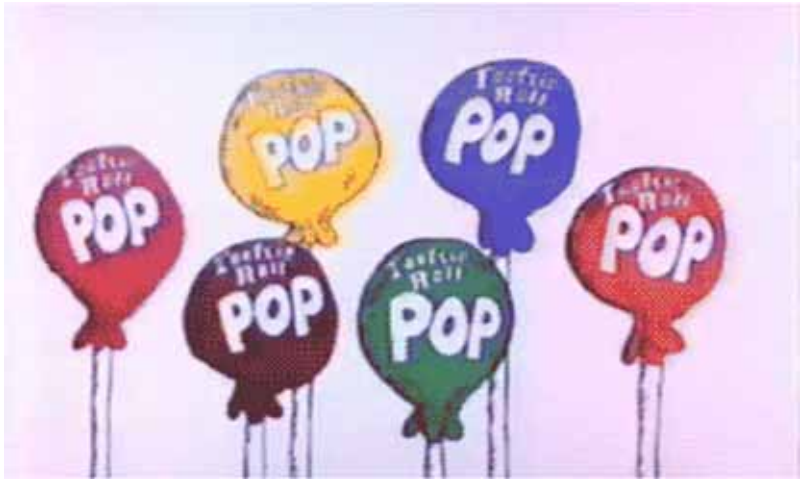
So limit them!

TYPES OF INFORMATION SECURITY CONTROLS



DEFENSE-IN-DEPTH

- Don’t be a Tootsie Roll Pop



SECURITY THROUGH OBSCURITY

- Hiding things is not a good control

CIS CRITICAL SECURITY CONTROLS

CSC 1 – Inventory of Authorized and Unauthorized Devices	CSC 2 – Inventory of Authorized and Unauthorized Software	CSC 3- Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4 – Continuous Vulnerability Assessment and Remediation	CSC 5 – Controlled Use of Administrative Privileges	CSC 6 – Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7 – Email and Web Browser Protections	CSC 8 – Malware Defenses	CSC 9 – Limitation and Control of Network, Ports, Protocols, and Services
CSC 10 – Data Recovery Capability	CSC 11 – Server Configurations for Network Devices such as Firewalls, Routers and Switches	CSC 12- Boundary Defense
CSC 13 – Data Protection	CSC 14 – Controlled Access Based on the Need to Know	CSC 15 – Wireless Access Controls
CSC 16 – Account Monitoring and Control	CSC 17 – Security Skills Assessment and Appropriate Training to Fill Gaps	CSC 18 – Application Software Security
CSC 19 – Incident Response and Management	CSC 20 – Penetration Tests and Red Team Exercises	Source: https://www.cisecurity.org/controls/

CIS CRITICAL SECURITY CONTROLS

CSC 1 – Inventory of Authorized and Unauthorized Devices	CSC 2 – Inventory of Authorized and Unauthorized Software	CSC 3- Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4 – Continuous Vulnerability Assessment and Remediation	CSC 5 – Controlled Use of Administrative Privileges	CSC 6 – Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7 – Email and Web Browser Protections	CSC 8 – Malware Defenses	CSC 9 – Limitation and Control of Network, Ports, Protocols, and Services
CSC 10 – Data Recovery Capability	CSC 11 – Server Configurations for Network Devices such as Firewalls, Routers and Switches	CSC 12- Boundary Defense
CSC 13 – Data Protection	CSC 14 – Controlled Access Based on the Need to Know	CSC 15 – Wireless Access Controls
CSC 16 – Account Monitoring and Control	CSC 17 – Security Skills Assessment and Appropriate Training to Fill Gaps	CSC 18 – Application Software Security
CSC 19 – Incident Response and Management	CSC 20 – Penetration Tests and Red Team Exercises	Source: https://www.cisecurity.org/controls/

OTHER NON-TECHNICAL CONTROLS

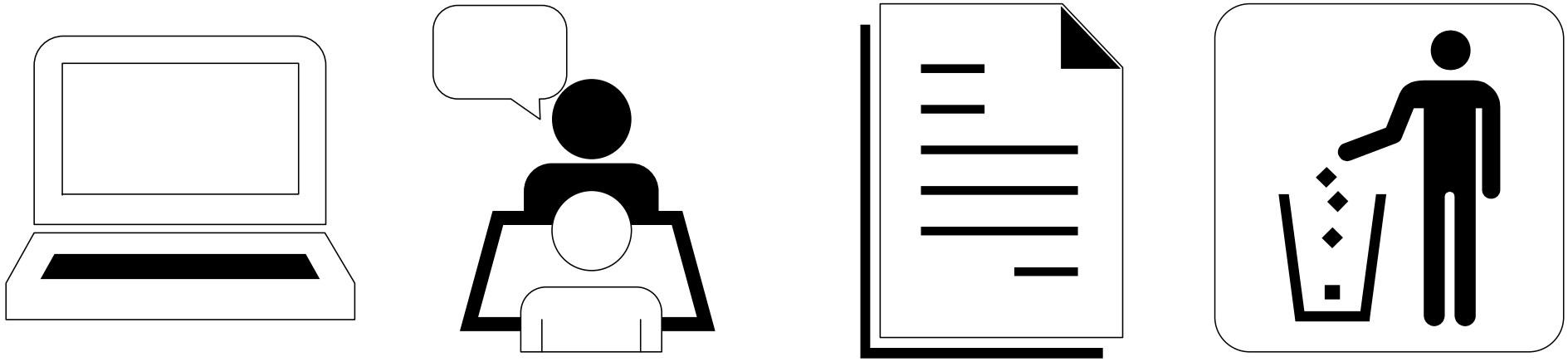
- Training & Awareness
- Separation of Duties
- Good Password Hygiene
- "Clean Desk" Policies
- Physical Security

SECURITY COMPLIANCE FRAMEWORKS

Compliance ≠ Security

CONCLUSION

INFORMATION IS EVERYWHERE



Information Security Has to Be Everywhere Too
(That Includes Every Audit)

QUESTIONS AND ANSWERS?

END OF PRESENTATION

THANK YOU FOR YOUR TIME AND ATTENTION!

IIA CHAPTER CHICAGO | 58TH ANNUAL SEMINAR