Managing Enterprise Cybersecurity MIS 4596

Human Element of Security

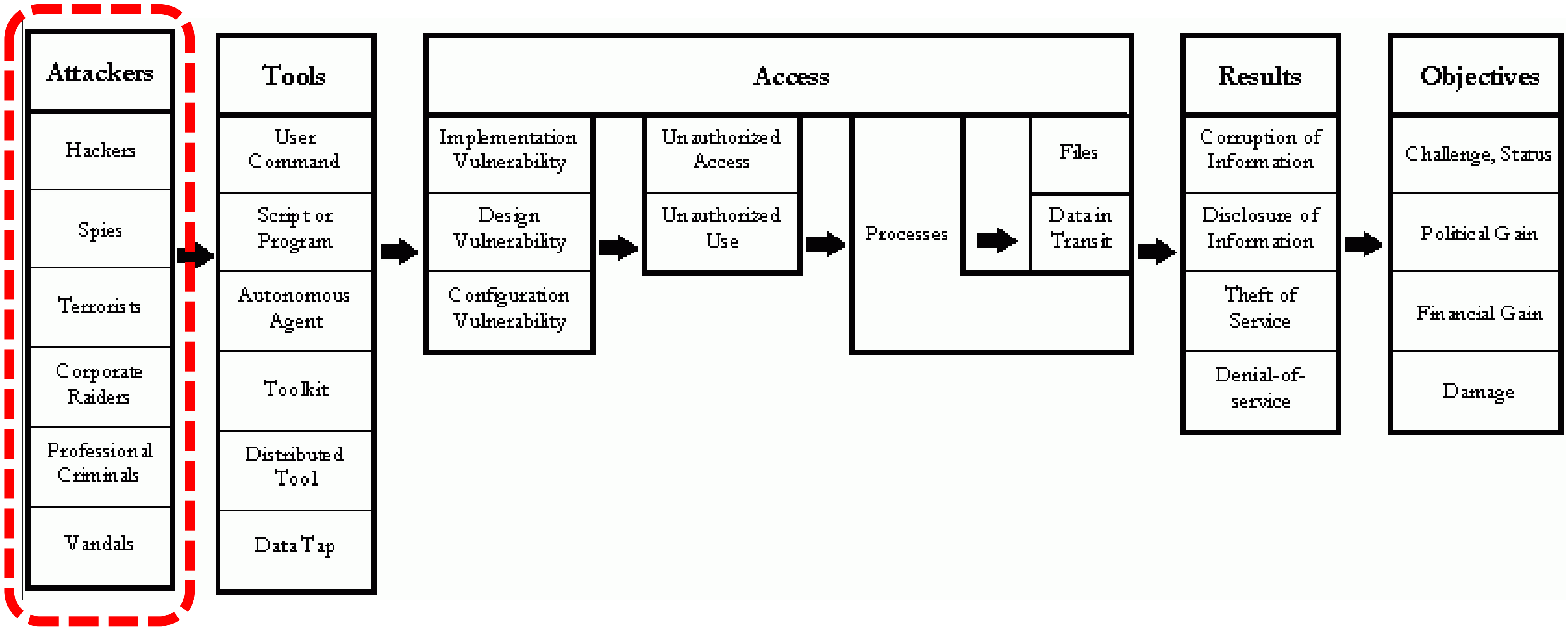
Unit #18

Agenda

- Human element of cyber security
- Employee risk
- Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs
- Social Engineering

What is in this picture ?

What is missing from this diagram?



Attackers: Hackers, Spies, Terrorists, Corporate Raiders, Professional Criminals, Vandals

Tools: User Command, Script or Program, Autonomous Agent, Toolkit, Distributed Tool, Data Tap

Access: Implementation Vulnerability, Design Vulnerability, Configuration Vulnerability; Unauthorized Access, Unauthorized Use; Processes; Files, Data in Transit

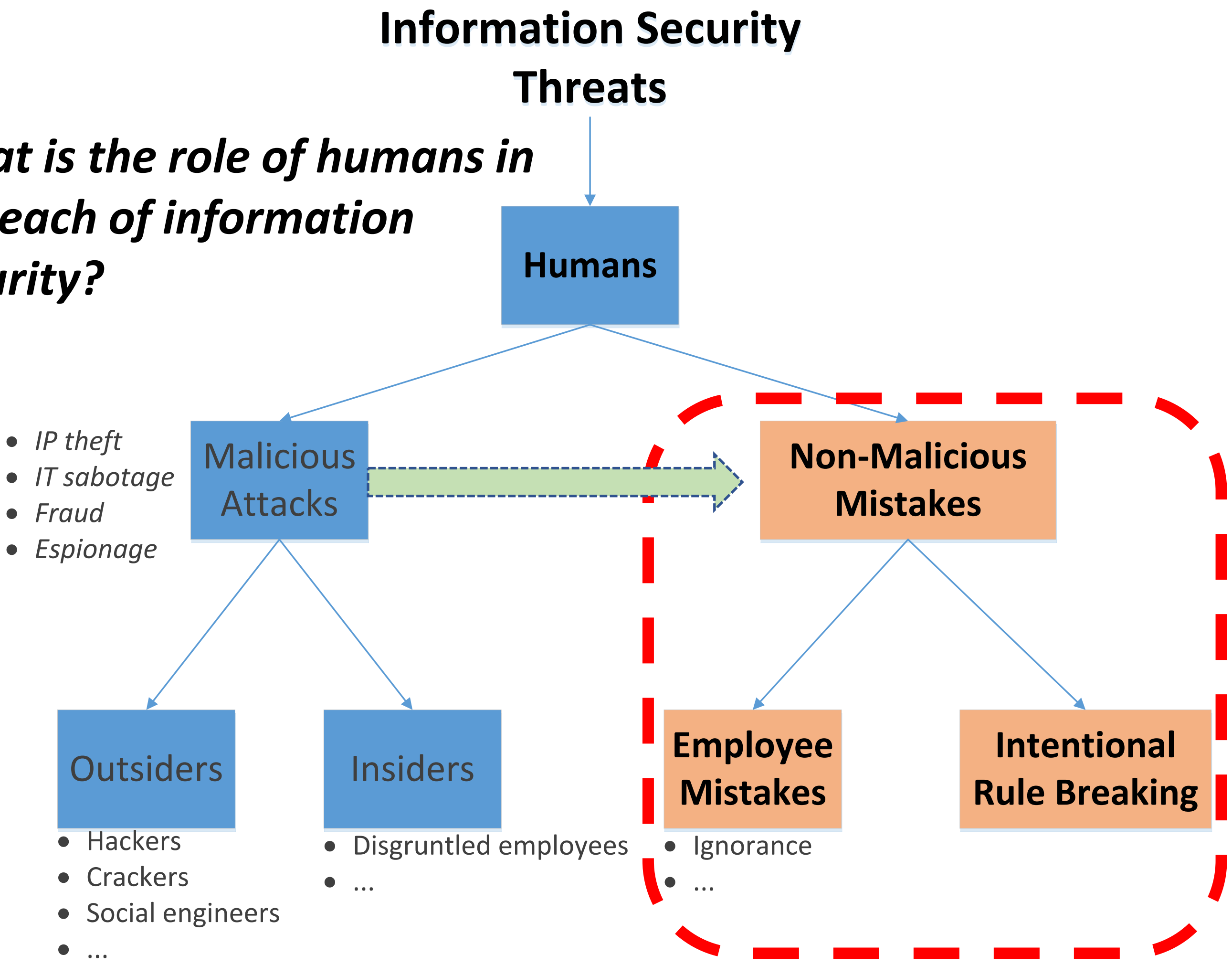
Results: Corruption of Information, Disclosure of Information, Theft of Service, Denial-of-service

Objectives: Challenge, Status, Political Gain, Financial Gain, Damage

Howard's process-based taxonomy, from Hansman, S. and Hunt, R., 2004, "A taxonomy of network and computer attacks", Computers & Security, page 3, Elsevier Ltd. Cited from Howard, JD, 1997, "An analysis of security incidents on the internet 1989-1995. PhD thesis, Carnegie Mellon University.

The threat landscape….

What is the role of humans in a breach of information security?



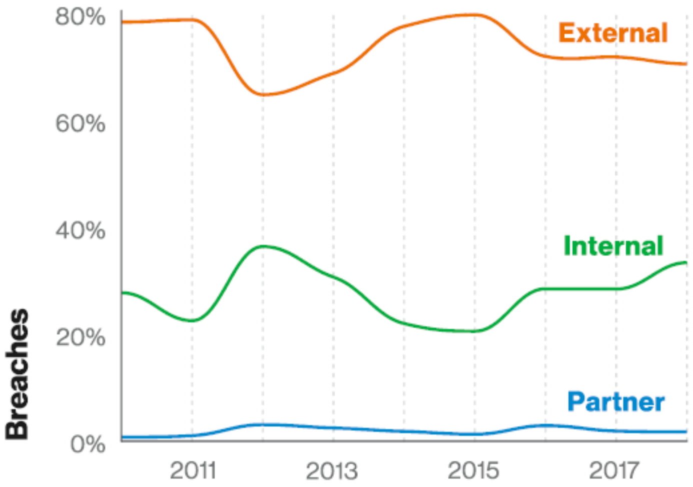
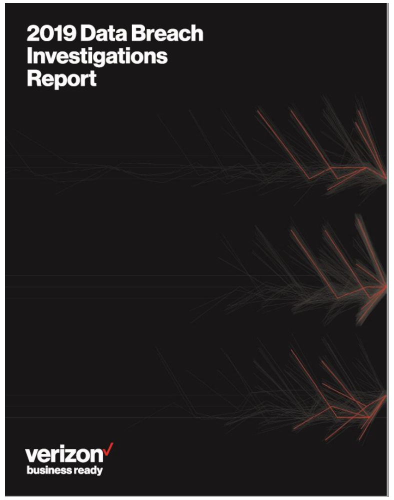
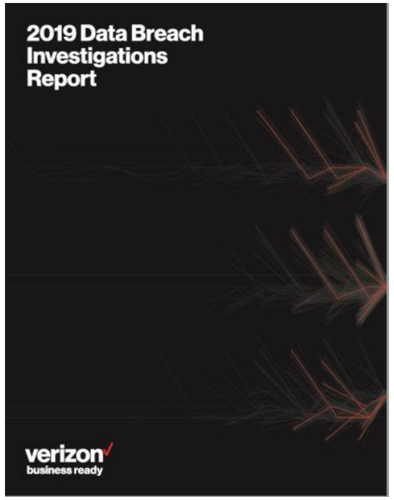


Figure 6. Threat actors in breaches over time


2019 Data Breach Investigations Report

verizon✓ business ready

What roles do employees play in these attack chains



2019 Data Breach Investigations Report

verizon✓
business ready

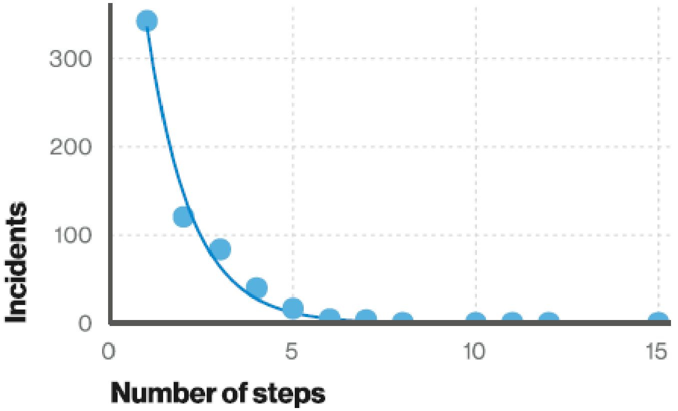


Figure 29. Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths.

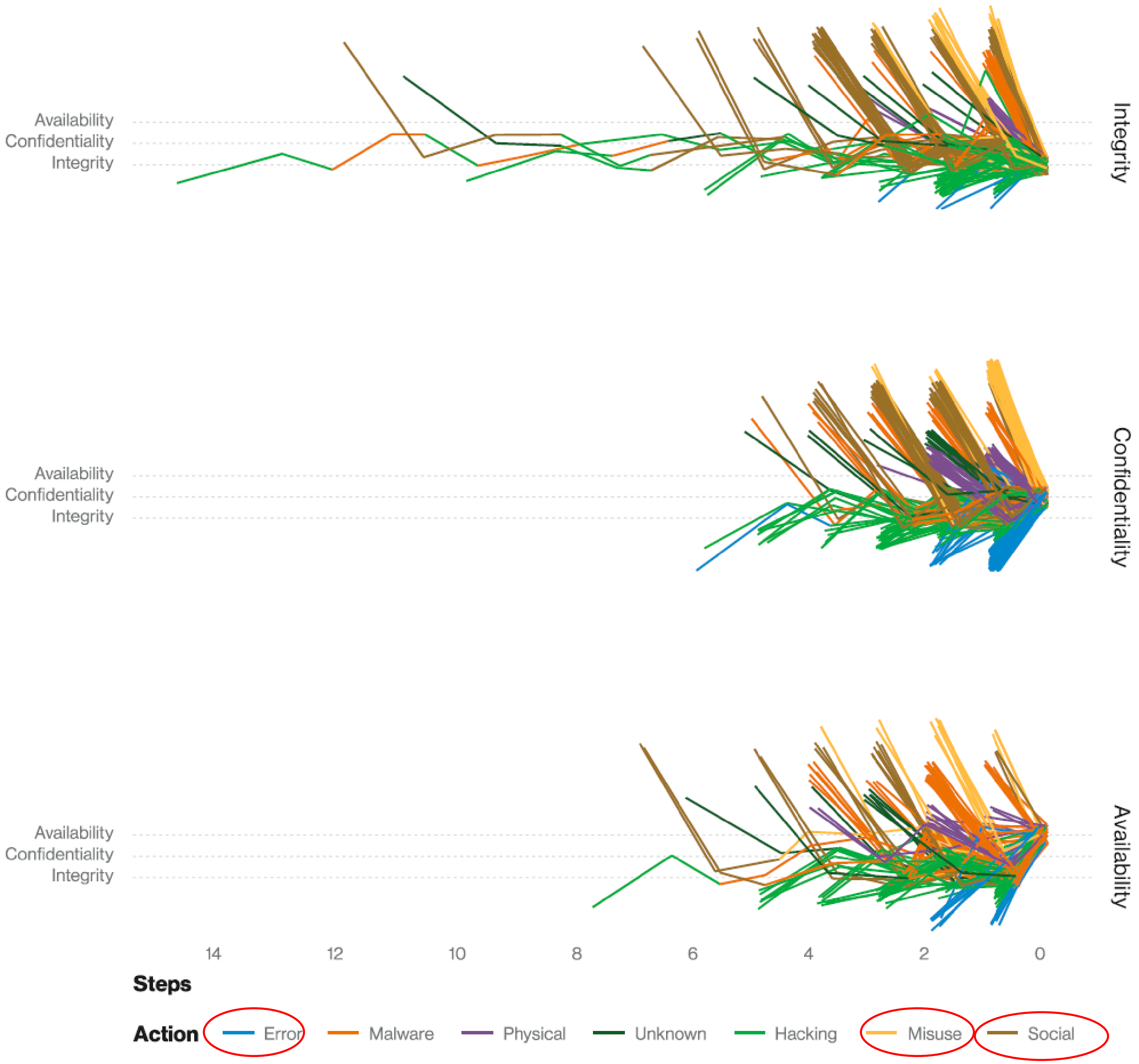
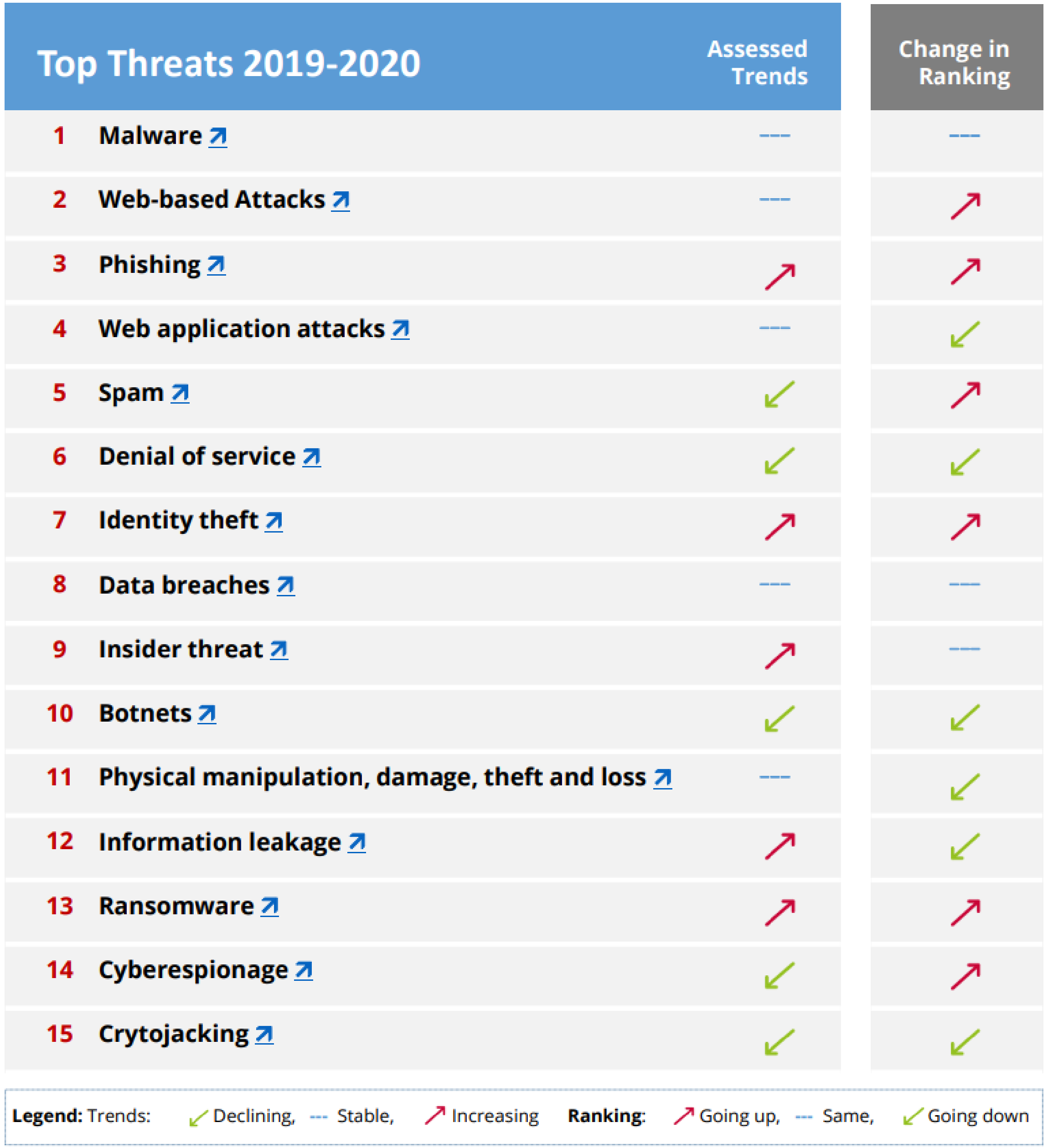


Figure 30. Attack chain by final attribute compromised[12] (n=941)



	Top Threats 2019-2020	Assessed Trends	Change in Ranking
1	Malware ↗	---	---
2	Web-based Attacks ↗	---	↗
3	Phishing ↗	↗	↗
4	Web application attacks ↗	---	↙
5	Spam ↗	↙	↗
6	Denial of service ↗	↙	↙
7	Identity theft ↗	↗	↗
8	Data breaches ↗	---	---
9	Insider threat ↗	↗	---
10	Botnets ↗	↙	↙
11	Physical manipulation, damage, theft and loss ↗	---	↙
12	Information leakage ↗	↗	↙
13	Ransomware ↗	↗	↗
14	Cyberespionage ↗	↙	↗
15	Crytojacking ↗	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking**: ↗ Going up, --- Same, ↙ Going down

enisa

From January 2019 to April 2020

The year in review

ENISA Threat Landscape

European Union Agency for Cybersecurity (ENISA)

In which of these threats are humans the vulnerability?

Employee Risk

- Ponemon Institute surveyed 1,000 small and medium-sized business owners, found negligent employees or contractors caused 60% of the data breaches
    - Employee training and stringent security protocols are necessary to mitigate risk of malicious insiders, otherwise danger of data breach remains high

- Ponemon survey of 612 CISOs found that 70% consider the “lack of competent in-house staff” as their top concern in 2018

Employee Risk

Verizon 2019 Data Breach Investigation Report

- 34% involved Internal actors
- 32% involved Phishing
- 21% caused by errors
- 15% caused by misuse by authorized users

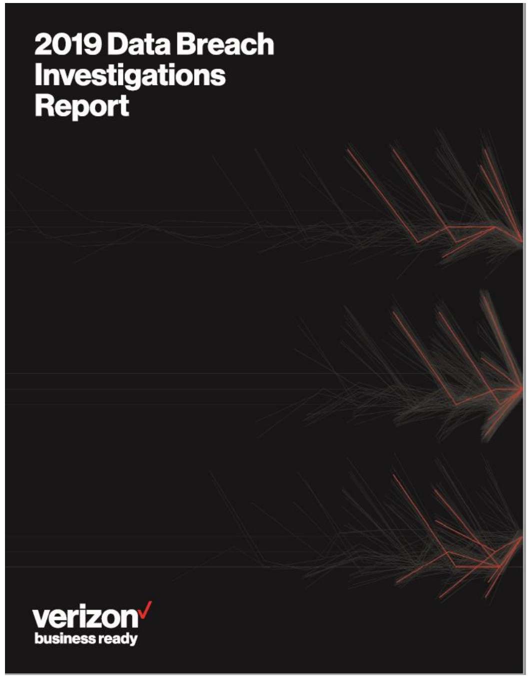
- Firewall and email filters to weed out phishing emails and malicious websites are important, but they're not enough
- Organizations must also ensure their security posture is good by:
  - Setting policies, educating staff, and enforcing good security hygiene
  - Taking advantage of the security options that are available
  - Training and testing employees
  - Implementing automated checks to ensure their security posture

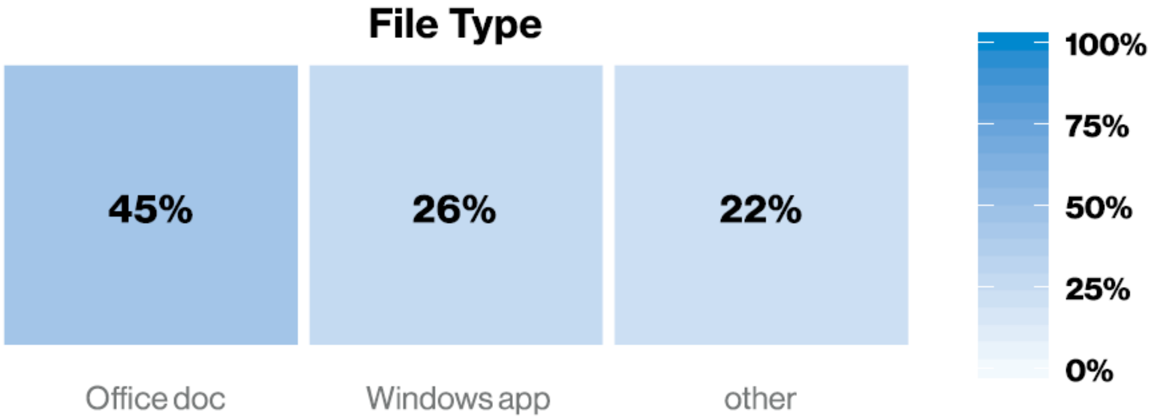
Employee Risk

Malware delivery methods

- “When the method of malware installation was known, email was the most common, email was the most common point of entry.”
  - ➢ Median company received 94% of detected malware by email

- Once introduced by email, additional malware is downloaded, often encoded to bypass detection and installed directly



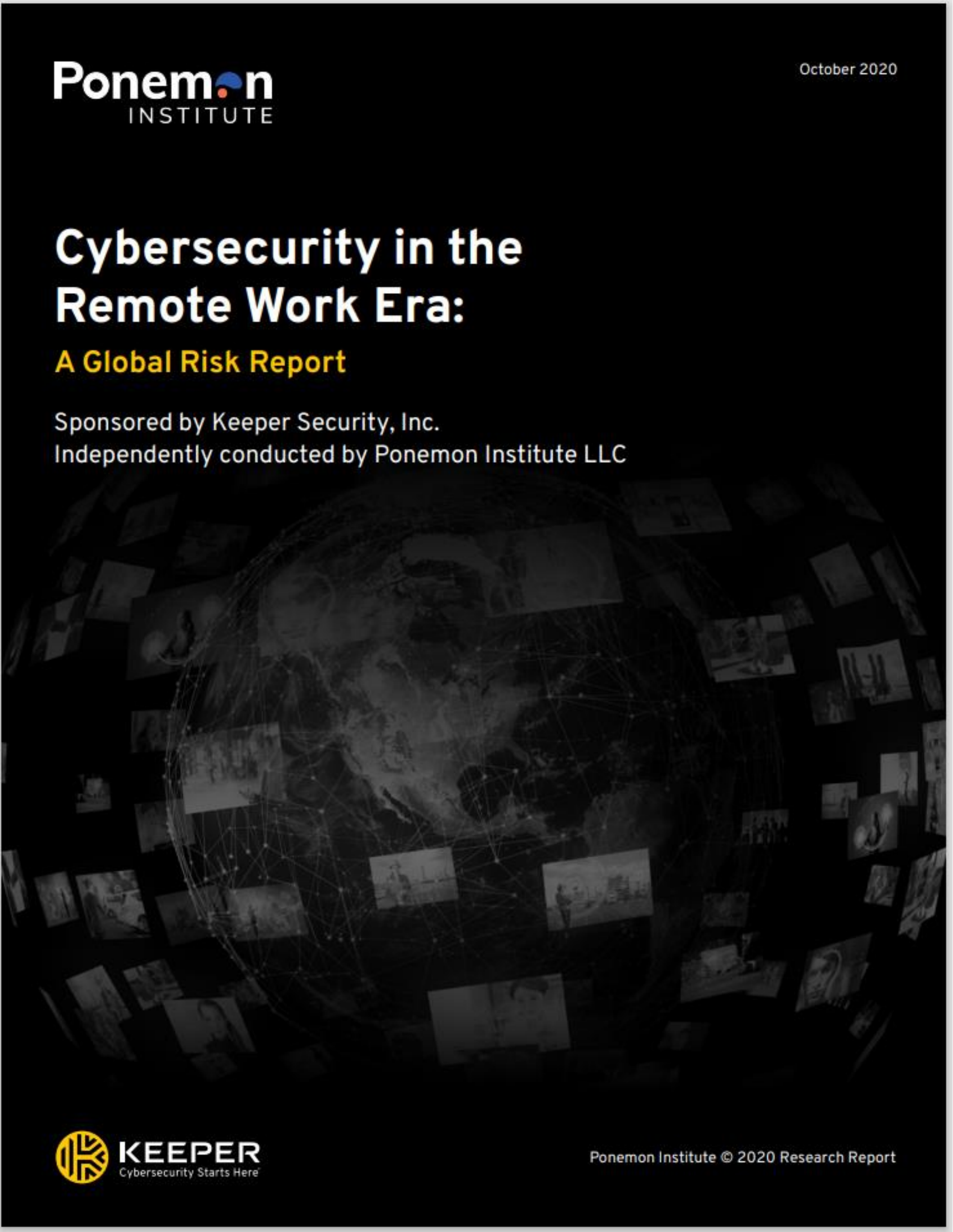


- 37% of breaches stole or used credentials
- Over 80% of breaches by hackers involve brute-force or use of lost or stolen credentials

DBIR

2020 Data Breach Investigations Report

verizon



Ponemon INSTITUTE

October 2020

Cybersecurity in the Remote Work Era:

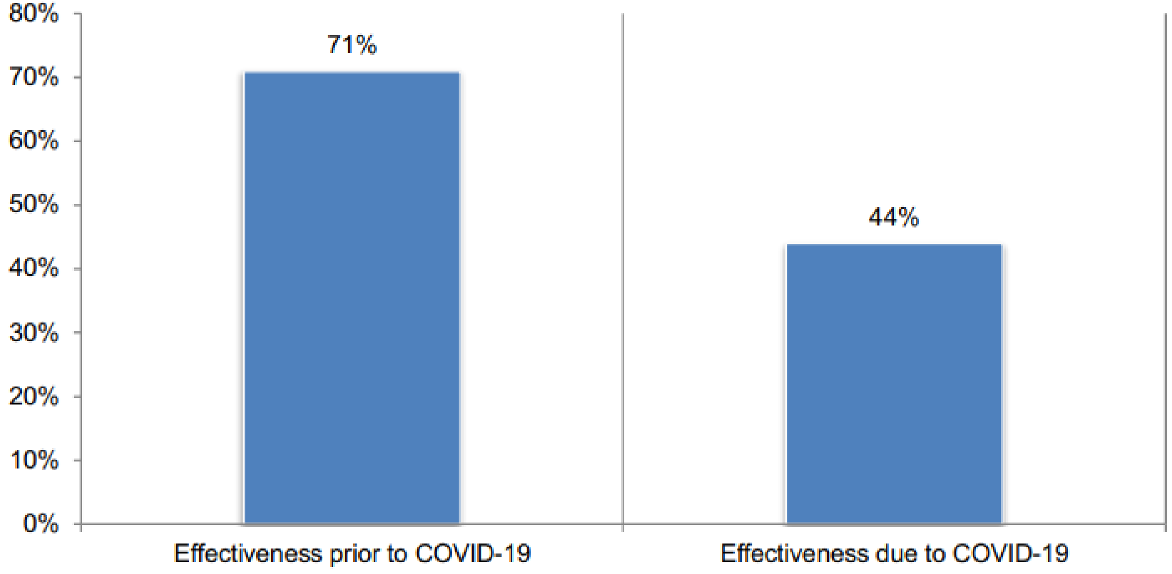
A Global Risk Report

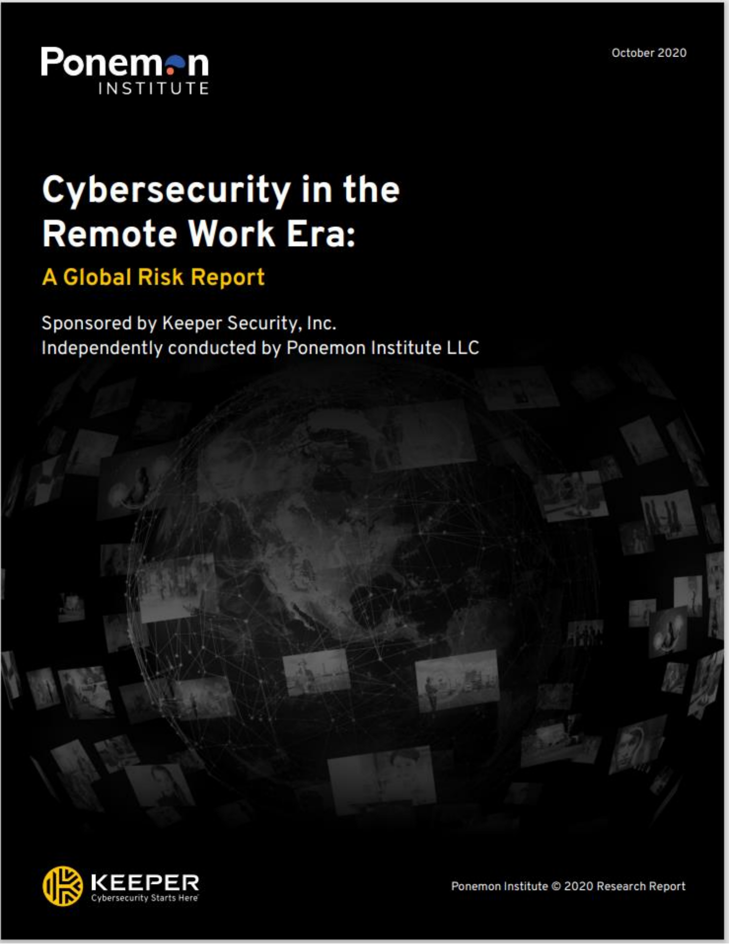
Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC

KEEPER
Cybersecurity Starts Here

Ponemon Institute © 2020 Research Report

Figure 1. Effectiveness of organizations' IT security posture prior to COVID-19 and due to COVID-19
1 = not effective to 10 = highly effective, 7+ responses presented





Ponemon INSTITUTE

October 2020

Cybersecurity in the Remote Work Era:

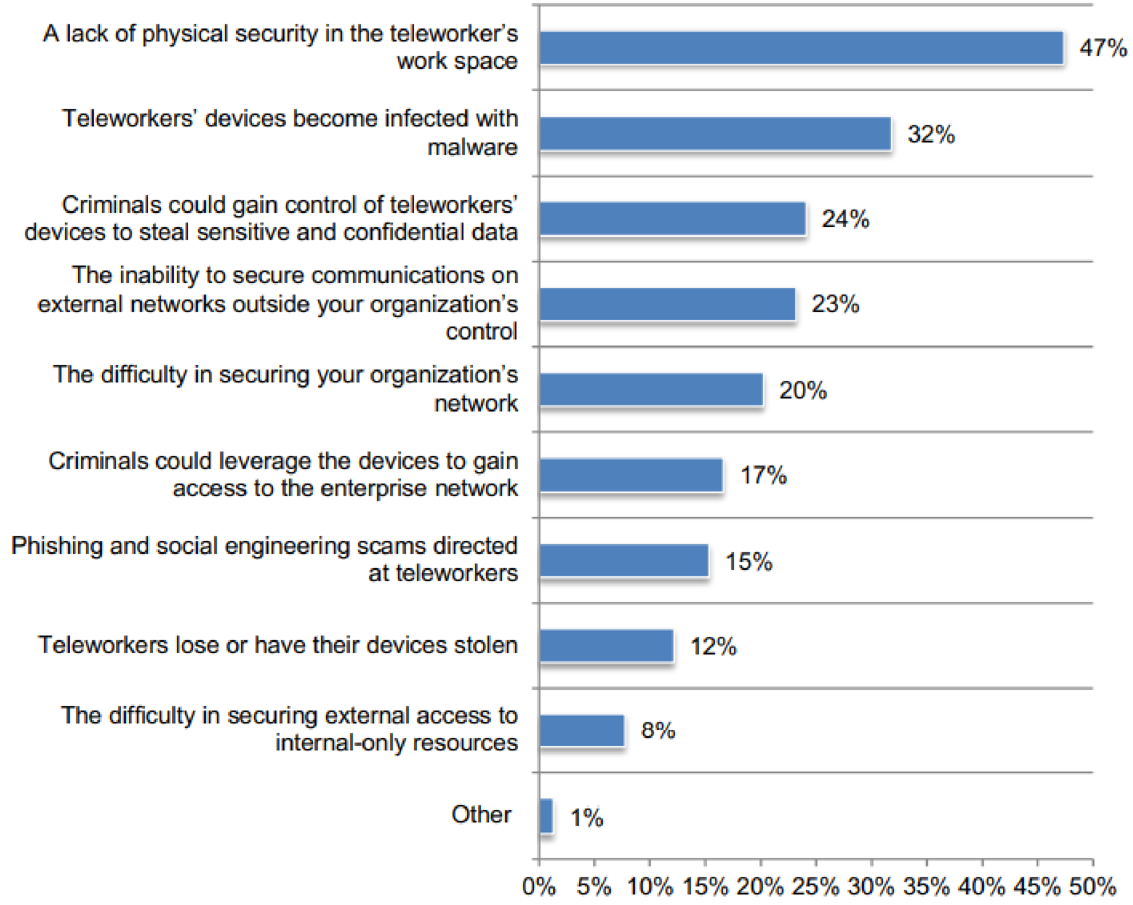
A Global Risk Report

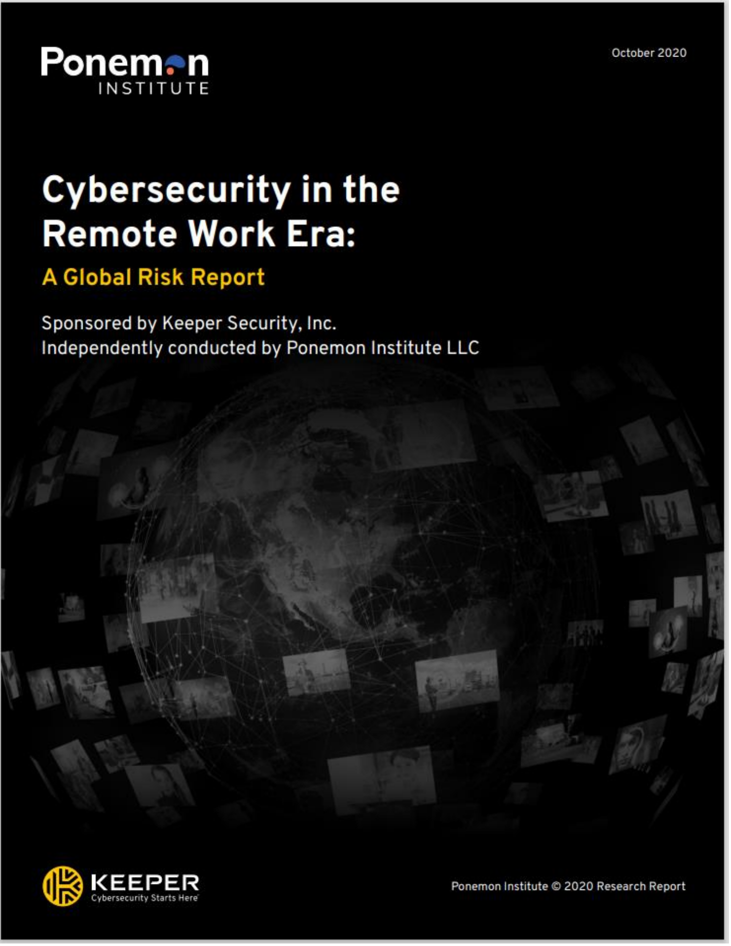
Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC

KEEPER
Cybersecurity Starts Here

Ponemon Institute © 2020 Research Report

Figure 3. Security risks organizations are most concerned about
More than one response permitted





Ponemon INSTITUTE

October 2020

Cybersecurity in the Remote Work Era:

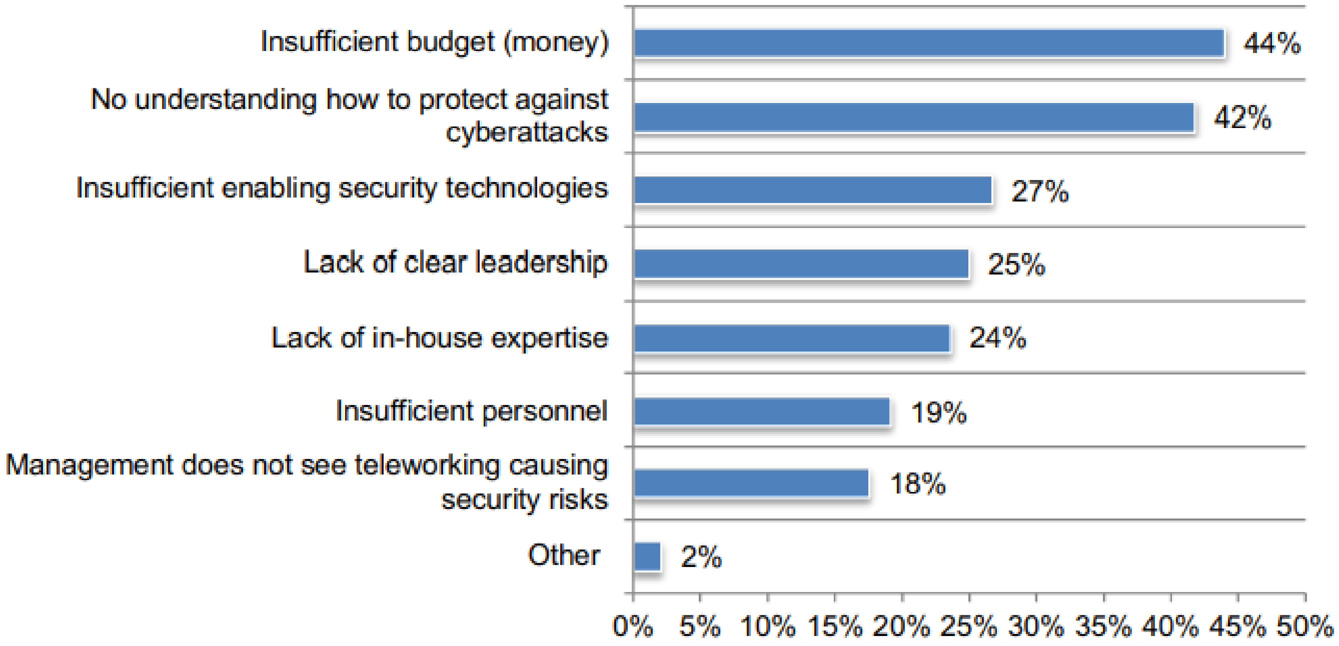
A Global Risk Report

Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC

KEEPER Cybersecurity Starts Here

Ponemon Institute © 2020 Research Report

Figure 5. What challenges keep your organization's IT security posture from being fully effective due to teleworking?
Two responses permitted



Why is teaching security awareness essential ?

- We have a culture of trust that can be taken advantage of with dubious intent
- Most people feel security is not part of their job
- People underestimate the value of information
- Security technologies give people a false sense of protection from attack

Non-malicious insider threat

1. A current or former employee, contractor, or business partner
2. Has or had authorized access to an organization’s network, system, or data
3. Through action or inaction without malicious intent…

   Causes harm or substantially increases the probability of future serious harm to…

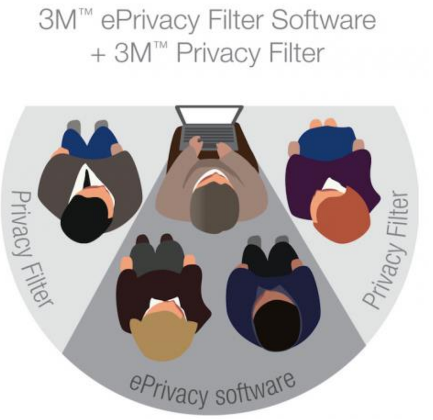
   confidentiality, integrity, or availability *of the organization’s information or information systems*

Major characteristic is ‘*failure in human performance*’

Carnegie Mellon Univeristy’s Software Engineering Institute’s
(SEI) Computer Emergency Response Team (CRT) CERT
Definition (2013)

The Unintentional Insider threat

from an add for…



“You spelled ‘confidential’ wrong.”

How would you characterize insiders' information security mistakes

- **Ignorant**
  - An unintentional accident
- **Negligent**
  - Willingly ignores policy to make things easier
- **Well meaning**
  - Prioritizes completing work and "getting 'er done" takes over following policy

Willis-Ford, C.D. (2015) "Education & Awareness: Manage the Insider Threat", SRA International Inc., FISSA (Federal Information Systems Security Awareness) Working Group

http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

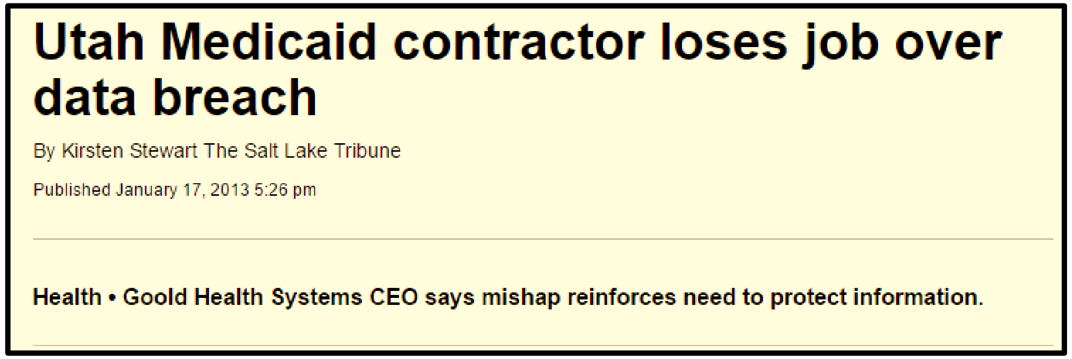
What are examples of insiders' accidents ?

- **Accidental Disclosure**
  - Posting sensitive data on public website
  - Sending sensitive data to wrong email address
- **Malicious Code**
  - Clicking on suspicious link in email
  - Using 'found' USB drive
- **Physical data release**
  - Losing paper records
- **Portable equipment**
  - Losing laptop, tablet
  - Losing portable storage device (USB drive, CD)

Willis-Ford, C.D. (2015) "Education & Awareness: Manage the Insider Threat", SRA International Inc., FISSA (Federal Information Systems Security Awareness) Working Group

http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

Example of an accident made by a well-meaning employee…



Utah Medicaid contractor loses job over data breach

By Kirsten Stewart The Salt Lake Tribune

Published January 17, 2013 5:26 pm

Health • Goold Health Systems CEO says mishap reinforces need to protect information.

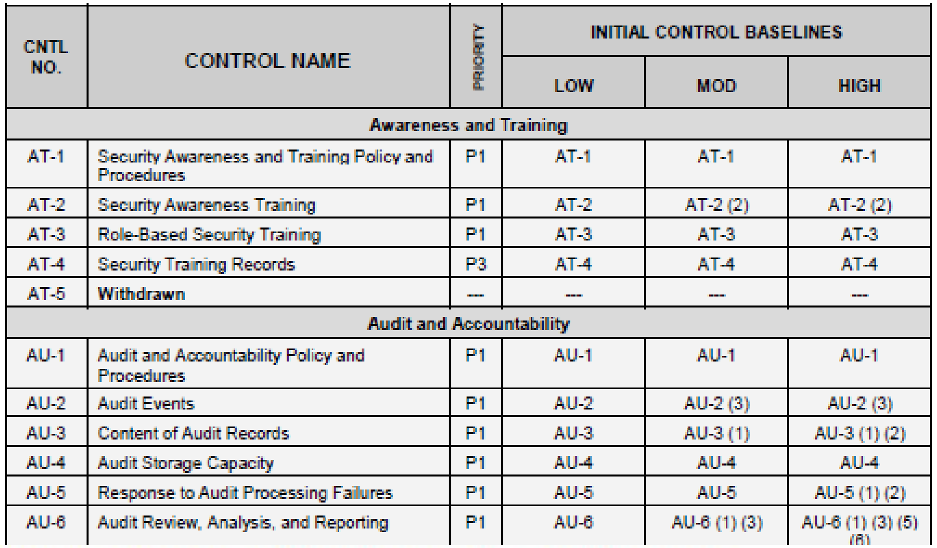
"Terrific employee":

- Account Manager handling health data for Utah
- Employee had trouble uploading a file requested by State Health Dept.
- Copied 6,000 medical records to USB drive
- Lost the USB drive, and reported the issue
- CEO admits the employee probably didn't even know she was breaking policy
  - this makes it accidental i.e. "well meaning…"

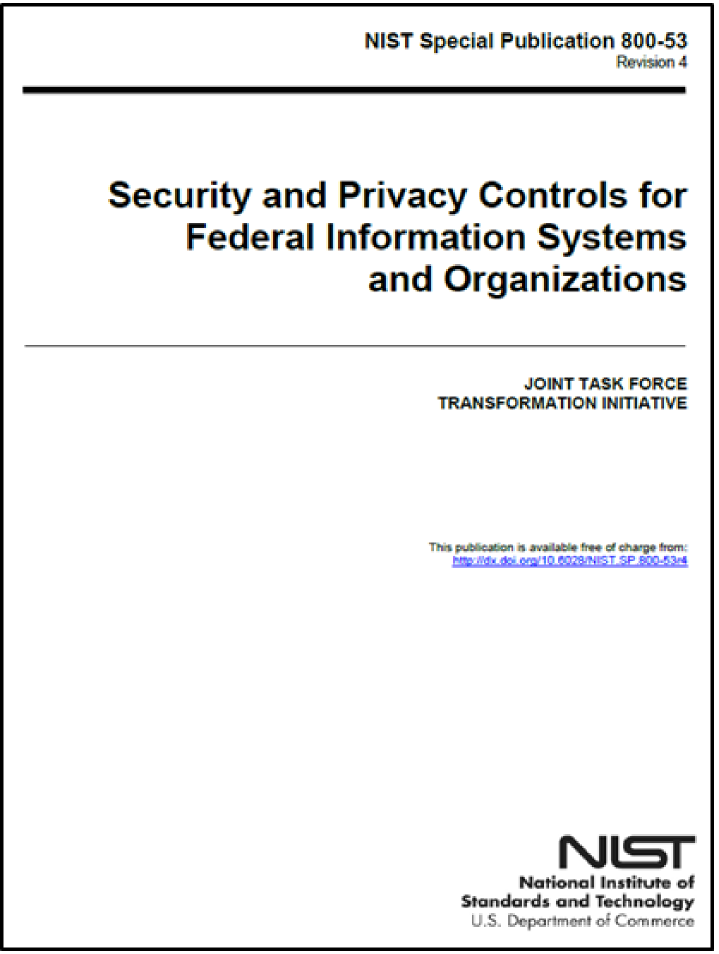
Agenda

- ✓Human element of cyber security
- ✓Employee risk
- Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs
- Social Engineering

Guidelines for employee cyber security Awareness and Training risk controls



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
	Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

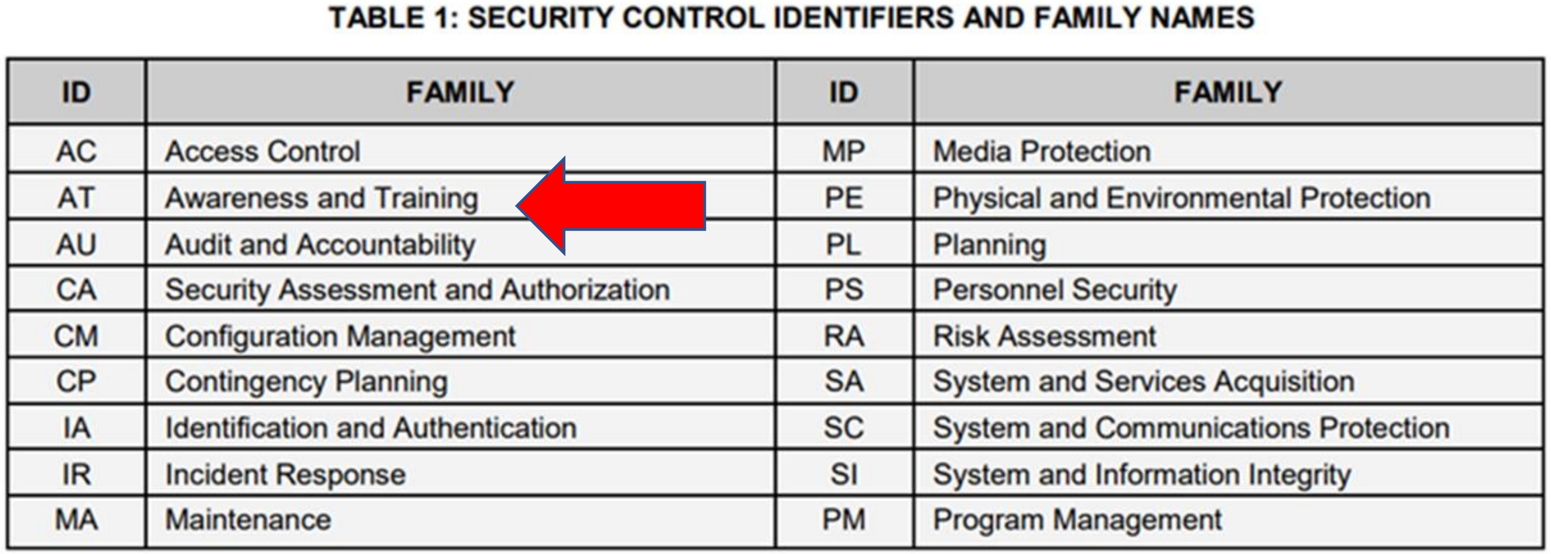
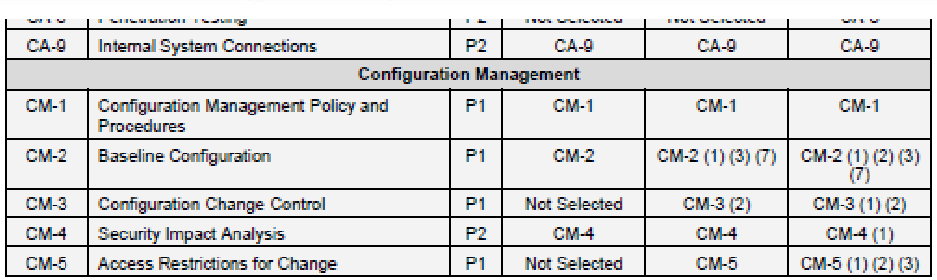
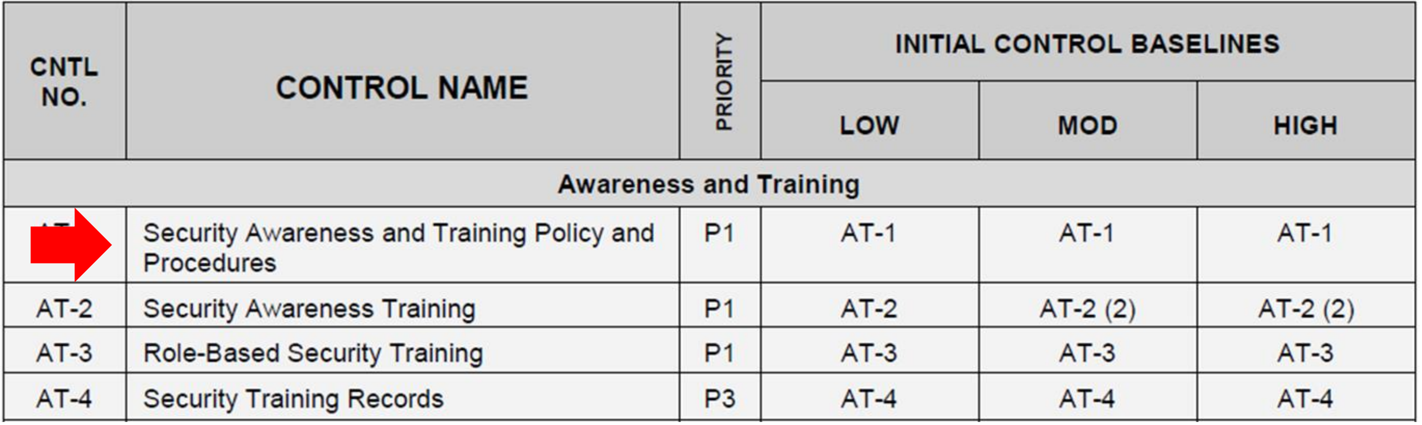


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

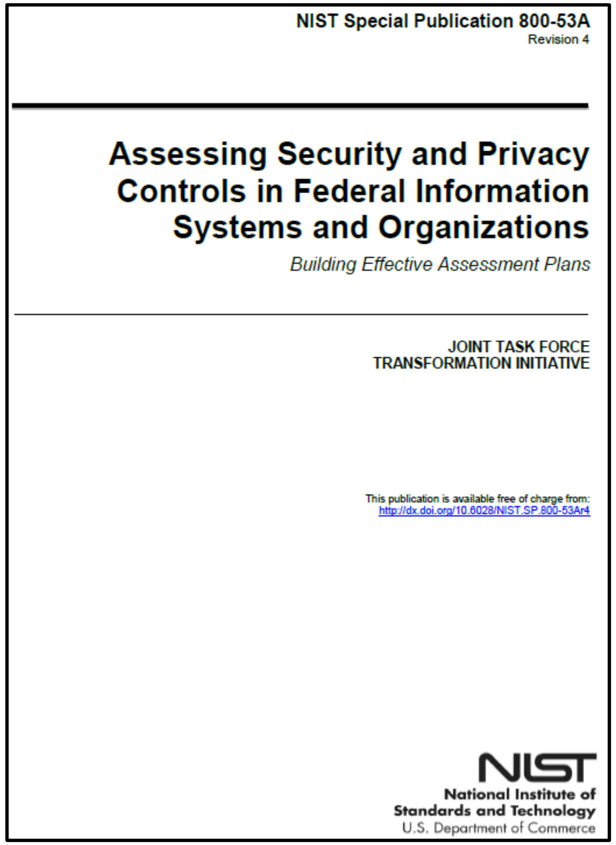


CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
	Configuration Management				
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
➡	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4

The guidelines for assessing cyber security risk controls



NIST Special Publication 800-53A
Revision 4

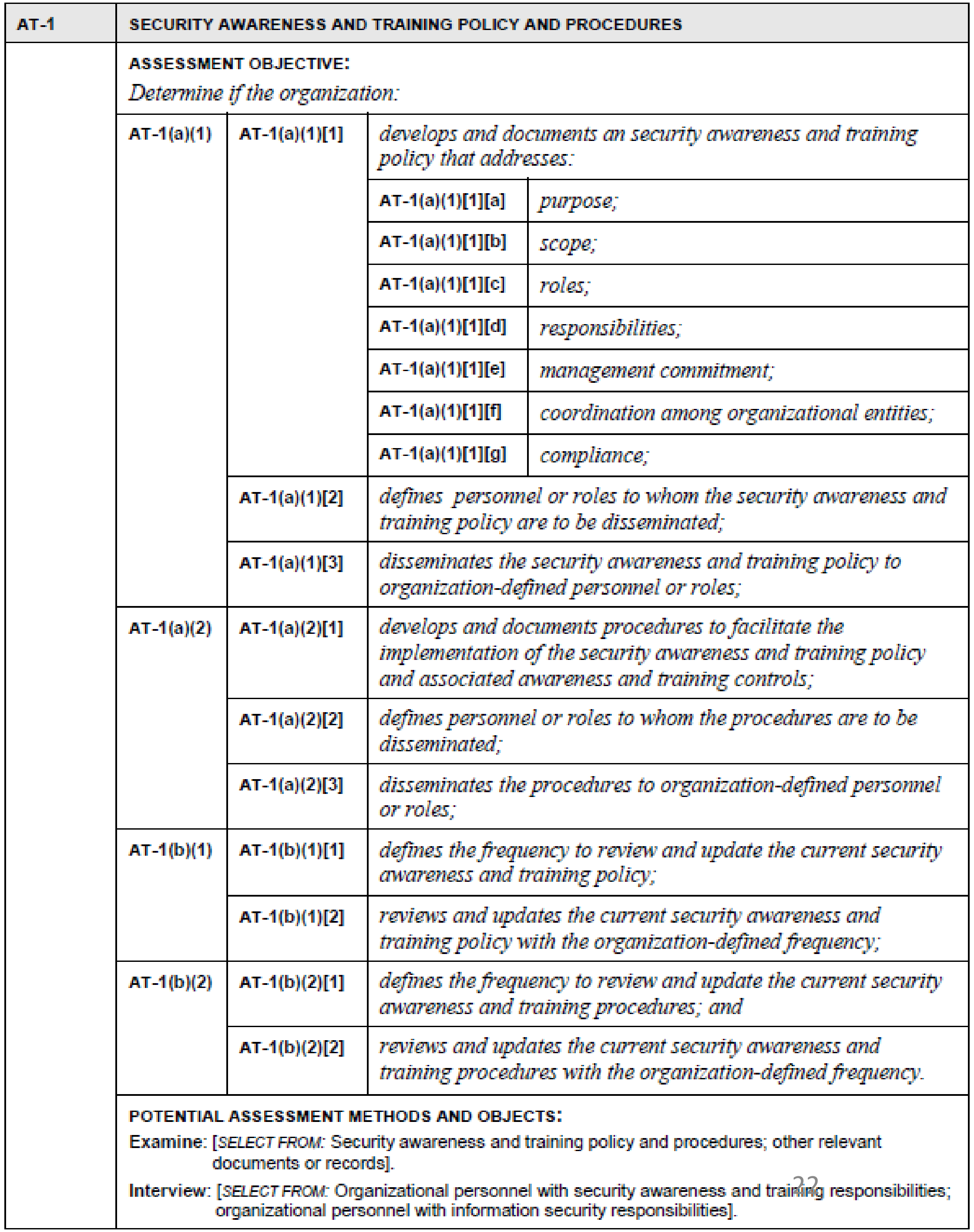
Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

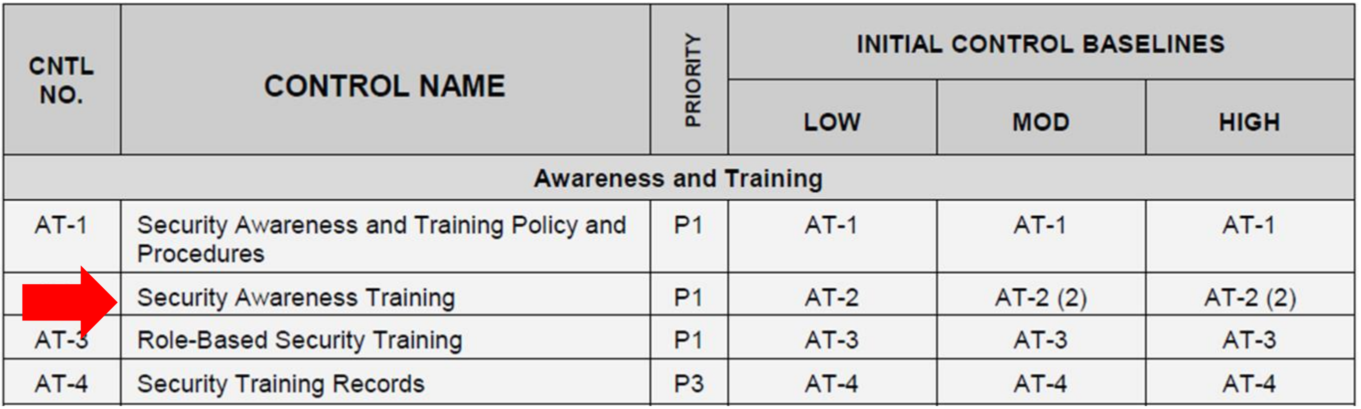


AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES			
	ASSESSMENT OBJECTIVE: *Determine if the organization:*			
	AT-1(a)(1)	AT-1(a)(1)[1]	*develops and documents an security awareness and training policy that addresses:*	
			AT-1(a)(1)[1][a]	*purpose;*
			AT-1(a)(1)[1][b]	*scope;*
			AT-1(a)(1)[1][c]	*roles;*
			AT-1(a)(1)[1][d]	*responsibilities;*
			AT-1(a)(1)[1][e]	*management commitment;*
			AT-1(a)(1)[1][f]	*coordination among organizational entities;*
			AT-1(a)(1)[1][g]	*compliance;*
		AT-1(a)(1)[2]	*defines personnel or roles to whom the security awareness and training policy are to be disseminated;*	
		AT-1(a)(1)[3]	*disseminates the security awareness and training policy to organization-defined personnel or roles;*	
	AT-1(a)(2)	AT-1(a)(2)[1]	*develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls;*	
		AT-1(a)(2)[2]	*defines personnel or roles to whom the procedures are to be disseminated;*	
		AT-1(a)(2)[3]	*disseminates the procedures to organization-defined personnel or roles;*	
	AT-1(b)(1)	AT-1(b)(1)[1]	*defines the frequency to review and update the current security awareness and training policy;*	
		AT-1(b)(1)[2]	*reviews and updates the current security awareness and training policy with the organization-defined frequency;*	
	AT-1(b)(2)	AT-1(b)(2)[1]	*defines the frequency to review and update the current security awareness and training procedures; and*	
		AT-1(b)(2)[2]	*reviews and updates the current security awareness and training procedures with the organization-defined frequency.*	

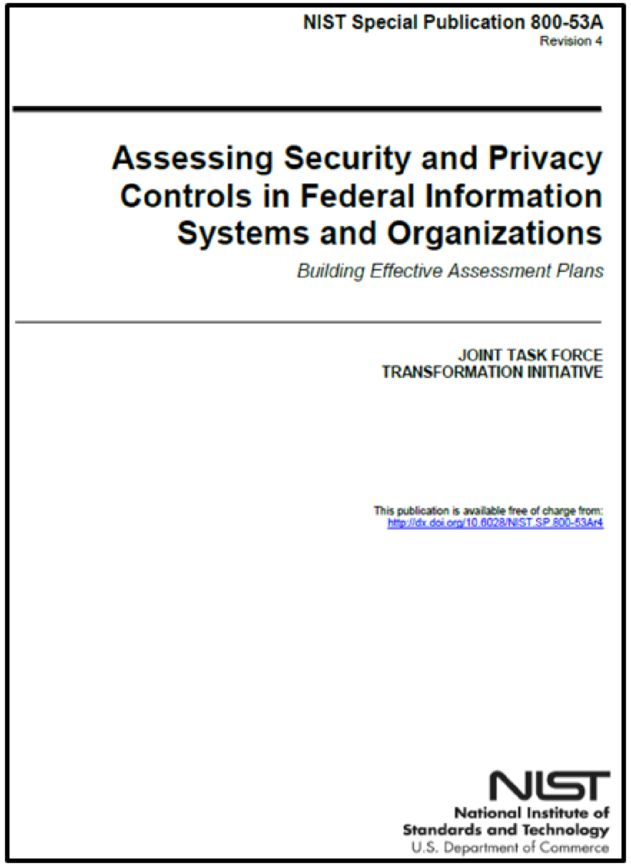
POTENTIAL ASSESSMENT METHODS AND OBJECTS:

Examine: [*SELECT FROM:* Security awareness and training policy and procedures; other relevant documents or records].

Interview: [*SELECT FROM:* Organizational personnel with security awareness and training responsibilities; organizational personnel with information security responsibilities].



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4



NIST Special Publication 800-53A
Revision 4

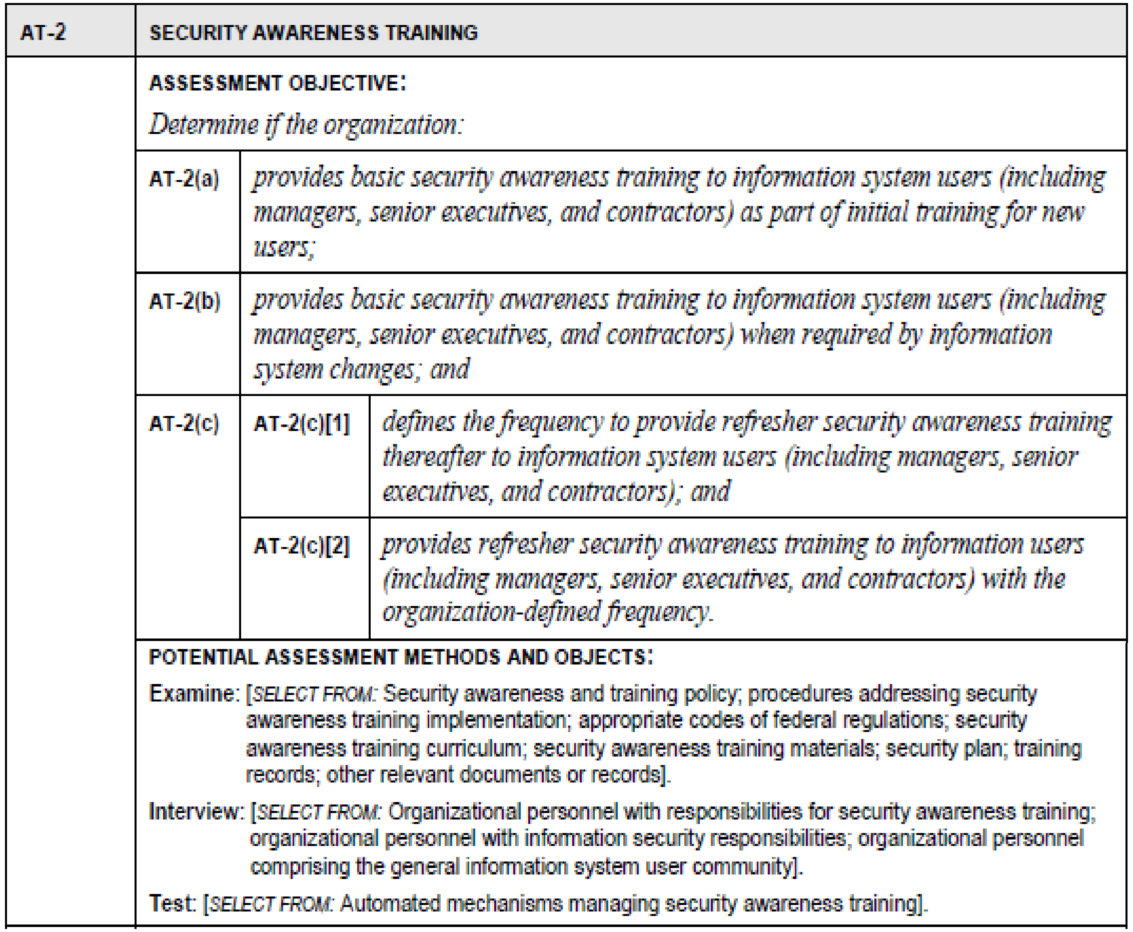
Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

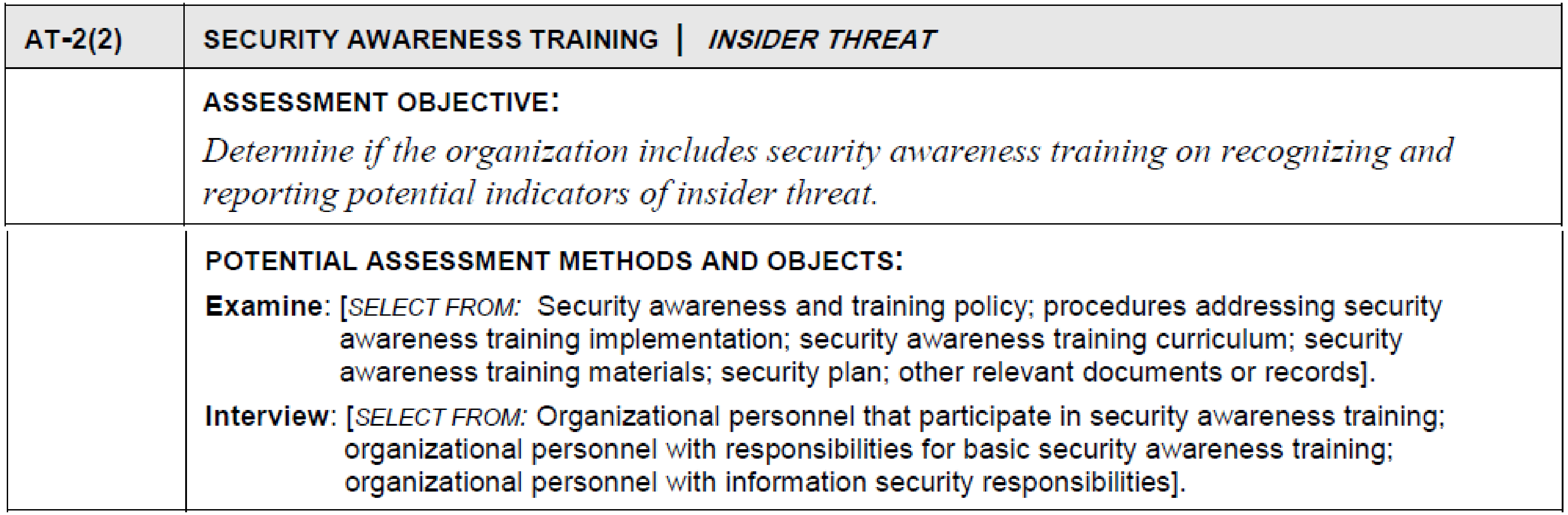
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



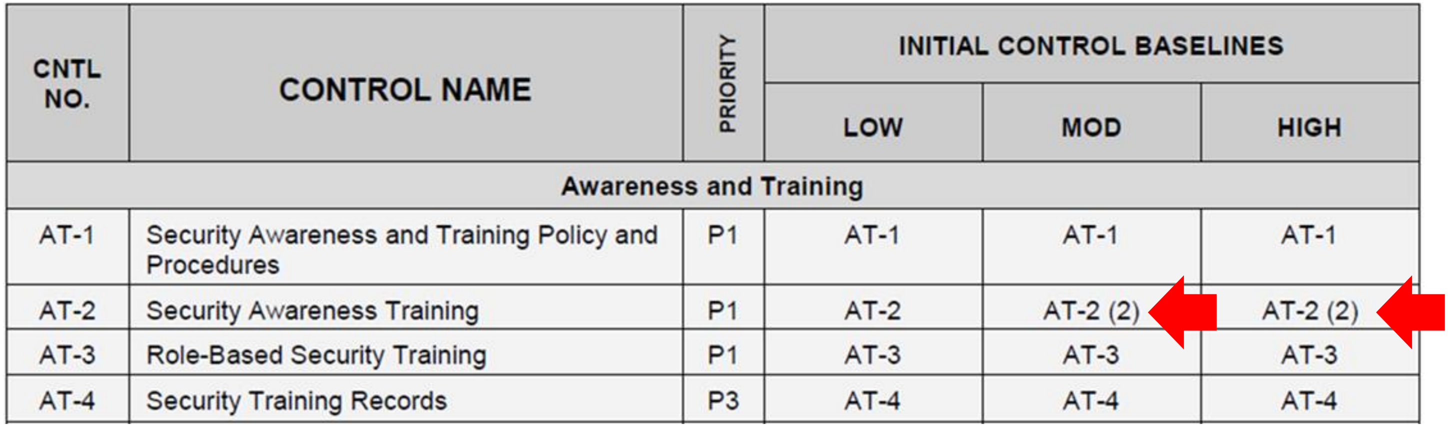
AT-2	SECURITY AWARENESS TRAINING		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	AT-2(a)	*provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users;*	
	AT-2(b)	*provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes; and*	
	AT-2(c)	AT-2(c)[1]	*defines the frequency to provide refresher security awareness training thereafter to information system users (including managers, senior executives, and contractors); and*
		AT-2(c)[2]	*provides refresher security awareness training to information users (including managers, senior executives, and contractors) with the organization-defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records]. Interview: [*SELECT FROM:* Organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities; organizational personnel comprising the general information system user community]. Test: [*SELECT FROM:* Automated mechanisms managing security awareness training].		

How do IT Auditors assess Security Awareness Training ?

Auditing a Security Awareness Training control enhancement



AT-2(2)	SECURITY AWARENESS TRAINING | *INSIDER THREAT*
	ASSESSMENT OBJECTIVE: *Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4

Agenda

✓Human element of cyber security

✓Employee risk

✓Cyber Security Employee Awareness and Training Risk Controls

- Evolution of Organizations’ Security Awareness and Training Programs
- Social Engineering

Why is teaching security awareness essential ?

- We have a culture of trust that can be taken advantage of with dubious intent
- Most people feel security is not part of their job
- People underestimate the value of information
- Security technologies give people a false sense of protection from attack

Non-malicious insider threat

1. A current or former employee, contractor, or business partner
2. Has or had authorized access to an organization's network, system, or data
3. Through action or inaction without malicious intent…

   Causes harm or substantially increases the probability of future serious harm to…

   confidentiality, integrity, or availability *of the organization's information or information systems*

Major characteristic is '*failure in human performance*'

Carnegie Mellon Univeristy's Software Engineering Institute's (SEI) Computer Emergency Response Team (CRT) CERT Definition (2013)

The Unintentional Insider threat

from an ad for…

3M™ ePrivacy Filter Software
+ 3M™ Privacy Filter

"You spelled 'confidential' wrong."

How would you characterize insiders’ information security mistakes

- **Ignorant**
  - An unintentional accident
- **Negligent**
  - Willingly ignores policy to make things easier
- **Well meaning**
  - Prioritizes completing work and “getting ‘er done” takes over following policy

Willis-Ford, C.D. (2015) “Education & Awareness: Manage the Insider Threat”, SRA International Inc., FISSA (Federal Information Systems Security Awareness) Working Group

http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

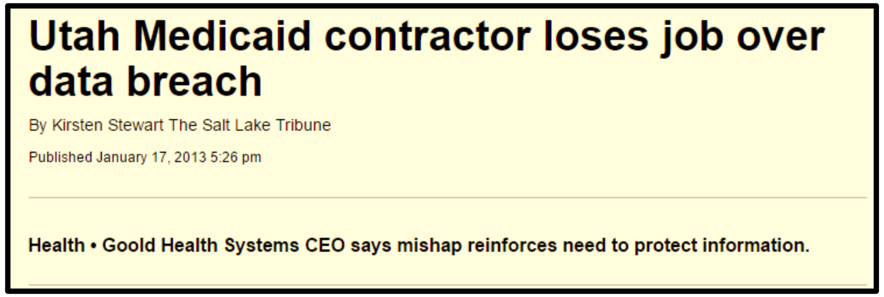
What are examples of insiders’ accidents ?

- **Accidental Disclosure**
  - Posting sensitive data on public website
  - Sending sensitive data to wrong email address
- **Malicious Code**
  - Clicking on suspicious link in email
  - Using ‘found’ USB drive
- **Physical data release**
  - Losing paper records
- **Portable equipment**
  - Losing laptop, tablet
  - Losing portable storage device (USB drive, CD)

Willis-Ford, C.D. (2015) “Education & Awareness: Manage the Insider Threat”, SRA International Inc., FISSA (Federal Information Systems Security Awareness) Working Group

http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-willis-ford.pdf

Example of an accident made by a well-meaning employee…



Utah Medicaid contractor loses job over data breach

By Kirsten Stewart The Salt Lake Tribune

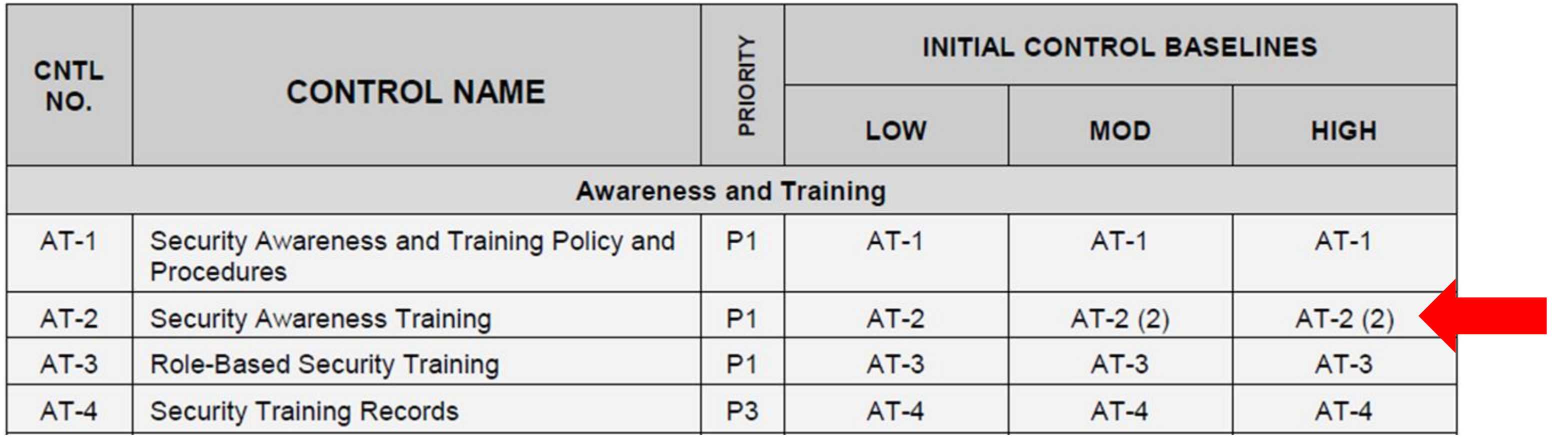
Published January 17, 2013 5:26 pm

Health • Goold Health Systems CEO says mishap reinforces need to protect information.

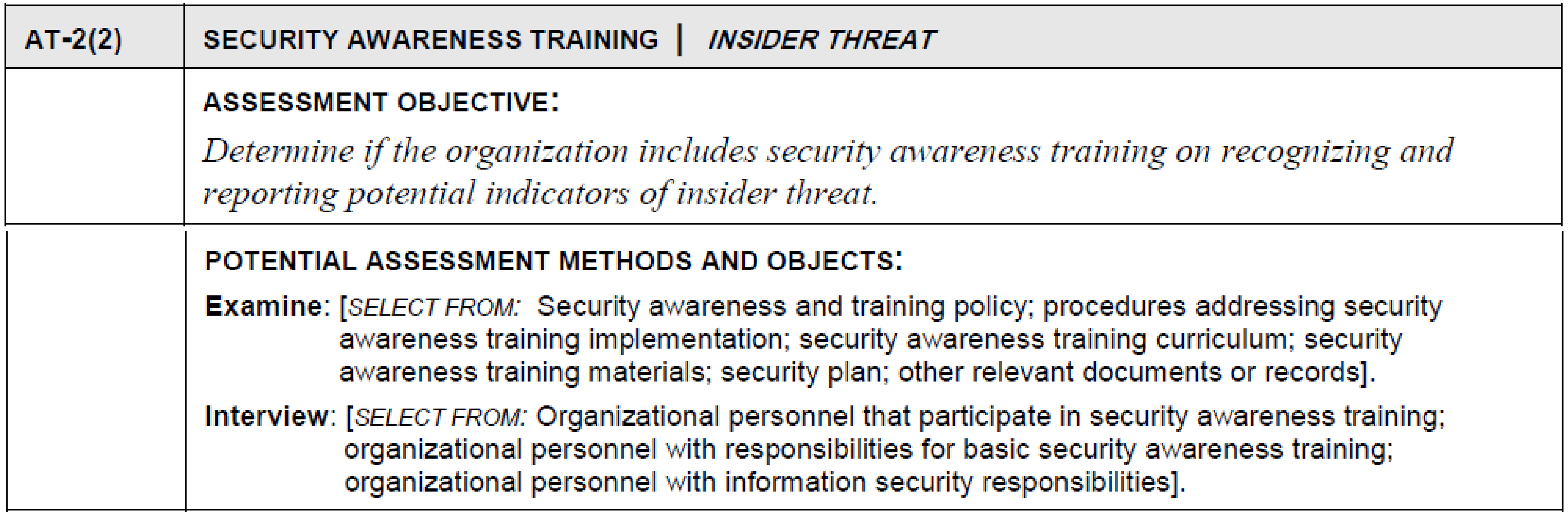
"Terrific employee":

- Account Manager handling health data for Utah
- Employee had trouble uploading a file requested by State Health Dept.
- Copied 6,000 medical records to USB drive
- Lost the USB drive, and reported the issue
- CEO admits the employee probably didn't even know she was breaking policy
  - this makes it accidental i.e. "well meaning…"

Auditing a Security Awareness Training control

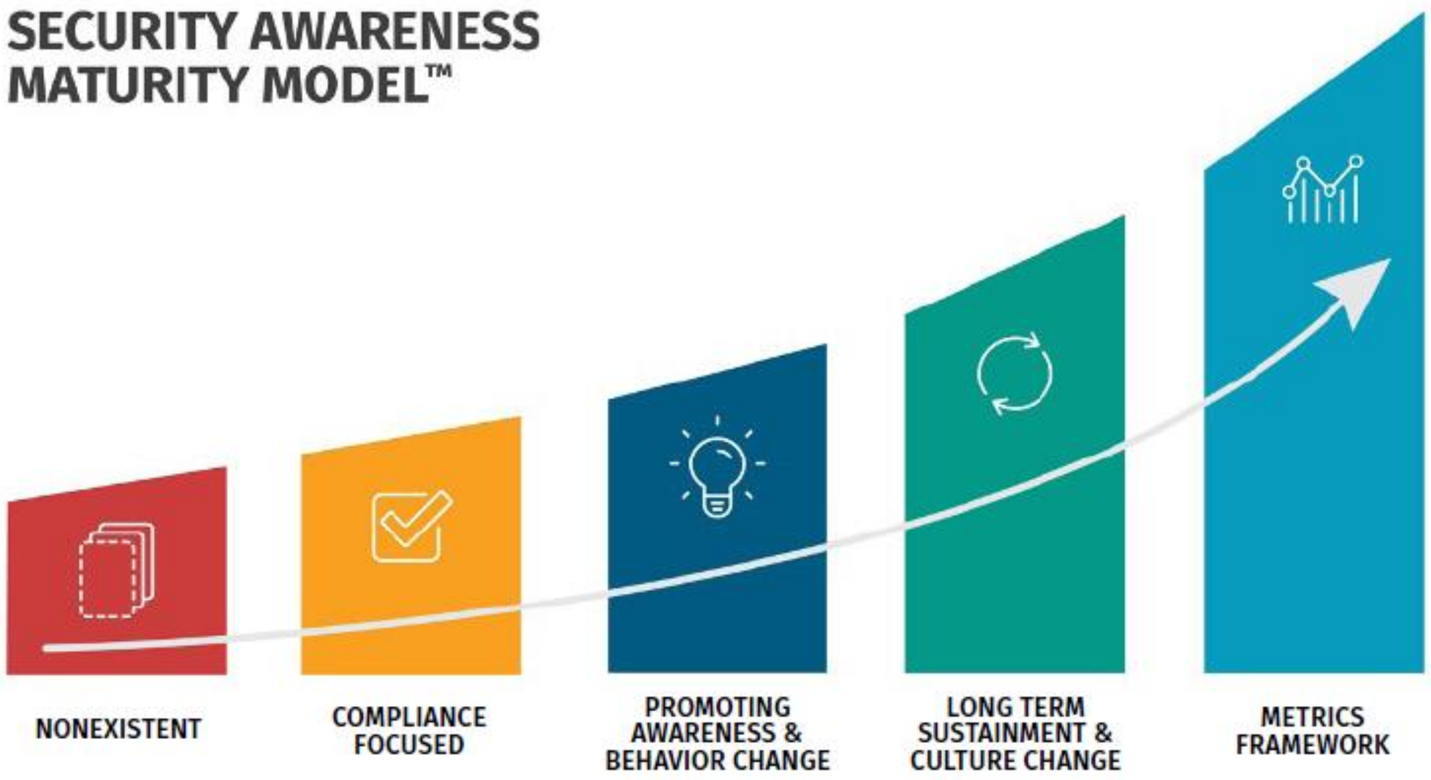


CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4



AT-2(2)	**SECURITY AWARENESS TRAINING | *INSIDER THREAT***
	ASSESSMENT OBJECTIVE: *Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].

What phases of security awareness do organizations go through as their programs mature?



SECURITY AWARENESS MATURITY MODEL™

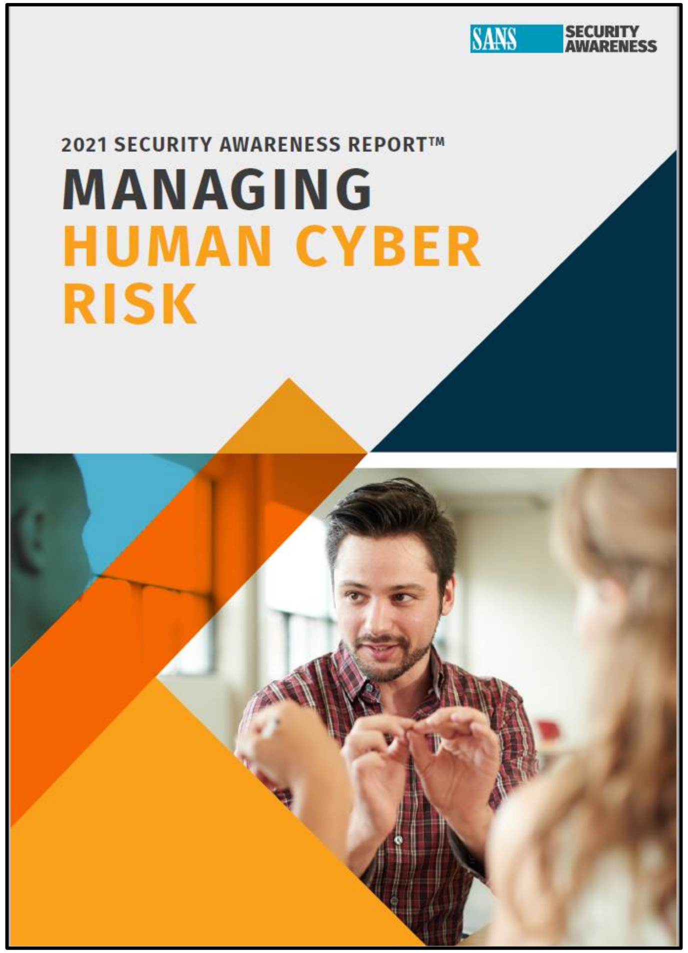
NONEXISTENT

COMPLIANCE FOCUSED

PROMOTING AWARENESS & BEHAVIOR CHANGE

LONG TERM SUSTAINMENT & CULTURE CHANGE

METRICS FRAMEWORK



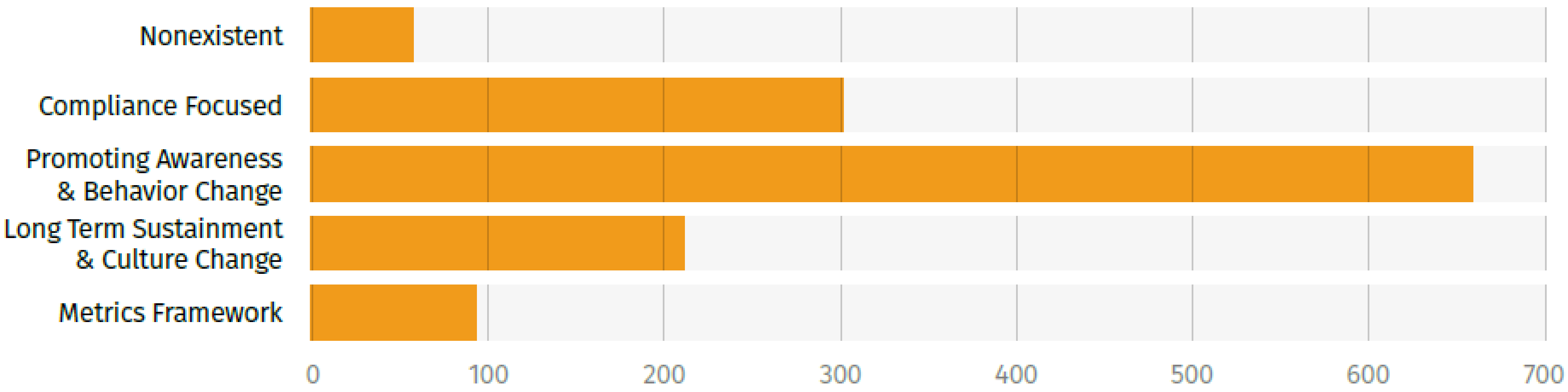
SANS SECURITY AWARENESS

2021 SECURITY AWARENESS REPORT™

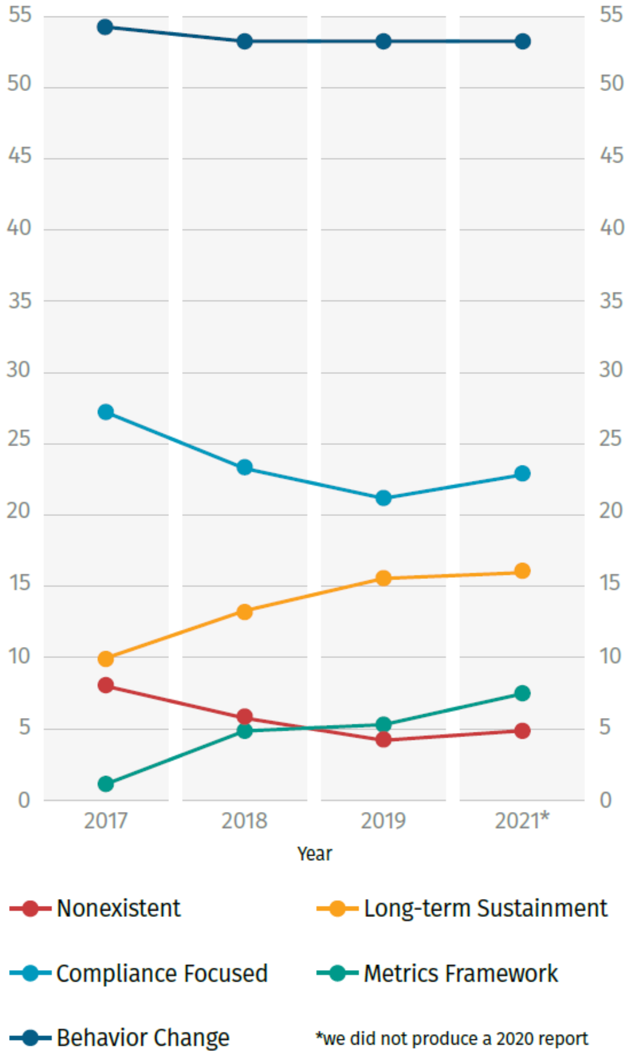
MANAGING HUMAN CYBER RISK

https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/

Benchmarking Maturity Levels



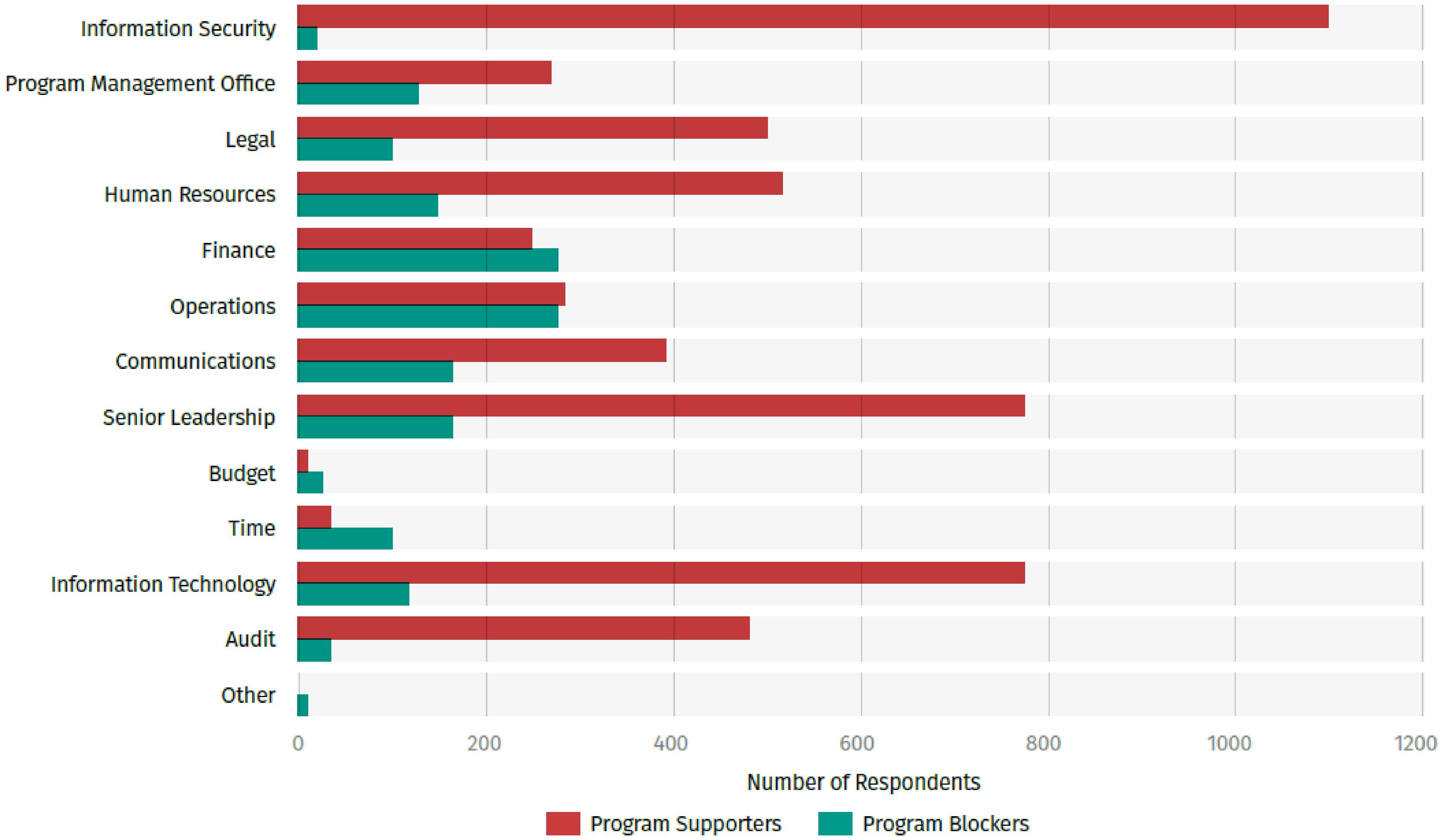
Program Maturity Over Time



*we did not produce a 2020 report

Reported Program Blockers and Supporters

SANS SECURITY AWARENESS



GAINING LEADERSHIP SUPPORT

Respondent data shows a correlation between executive support and program maturity. As organizational leaders often decide on critical program resourcing, identification of program goals, training time allocation, and program enforceability, executive support is a key ingredient in program success.

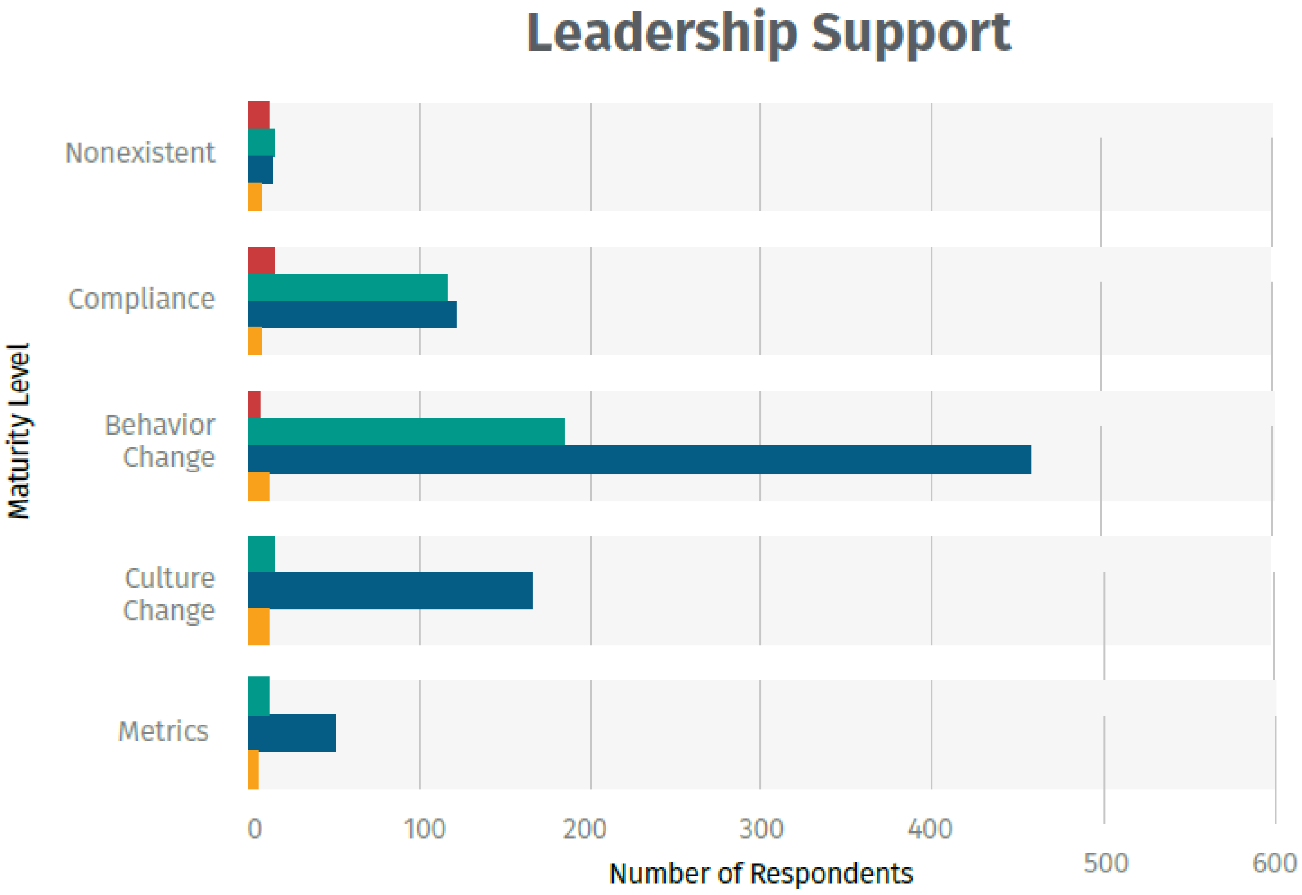
Support Level

🟥 I have no support

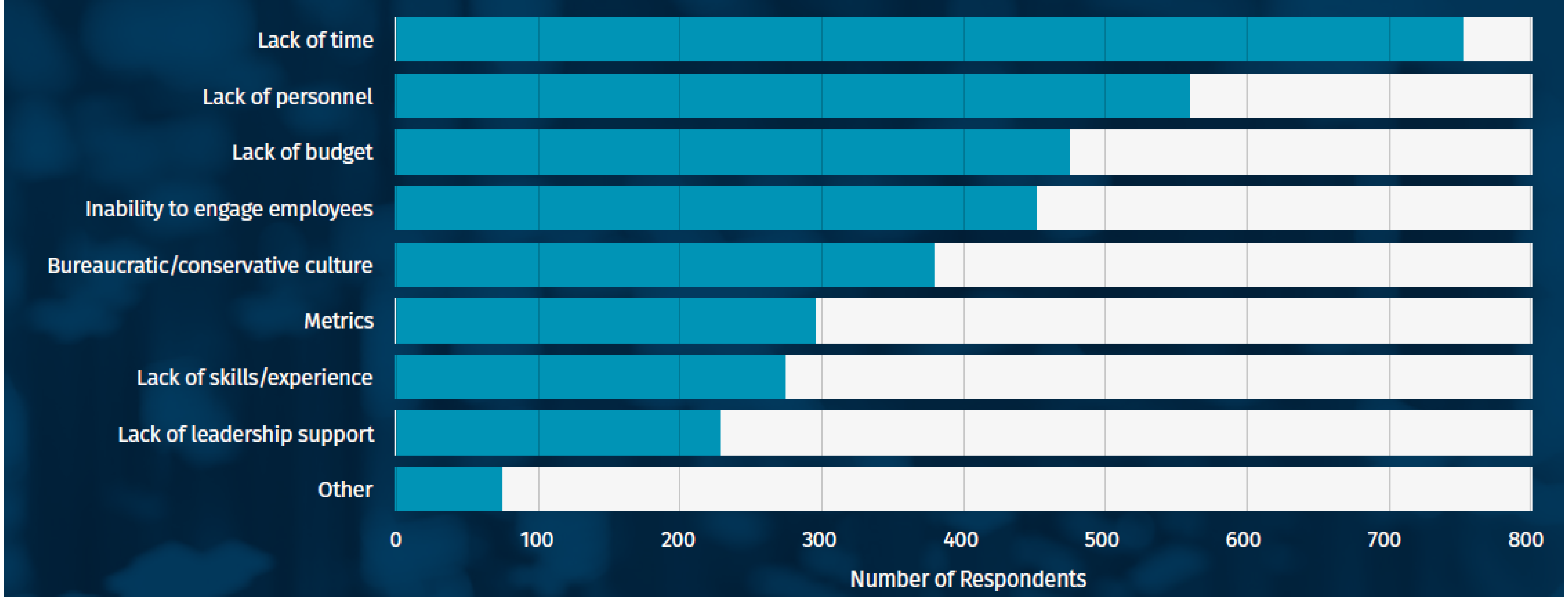
🟩 I have less support than I need

🟦 I have the support I need

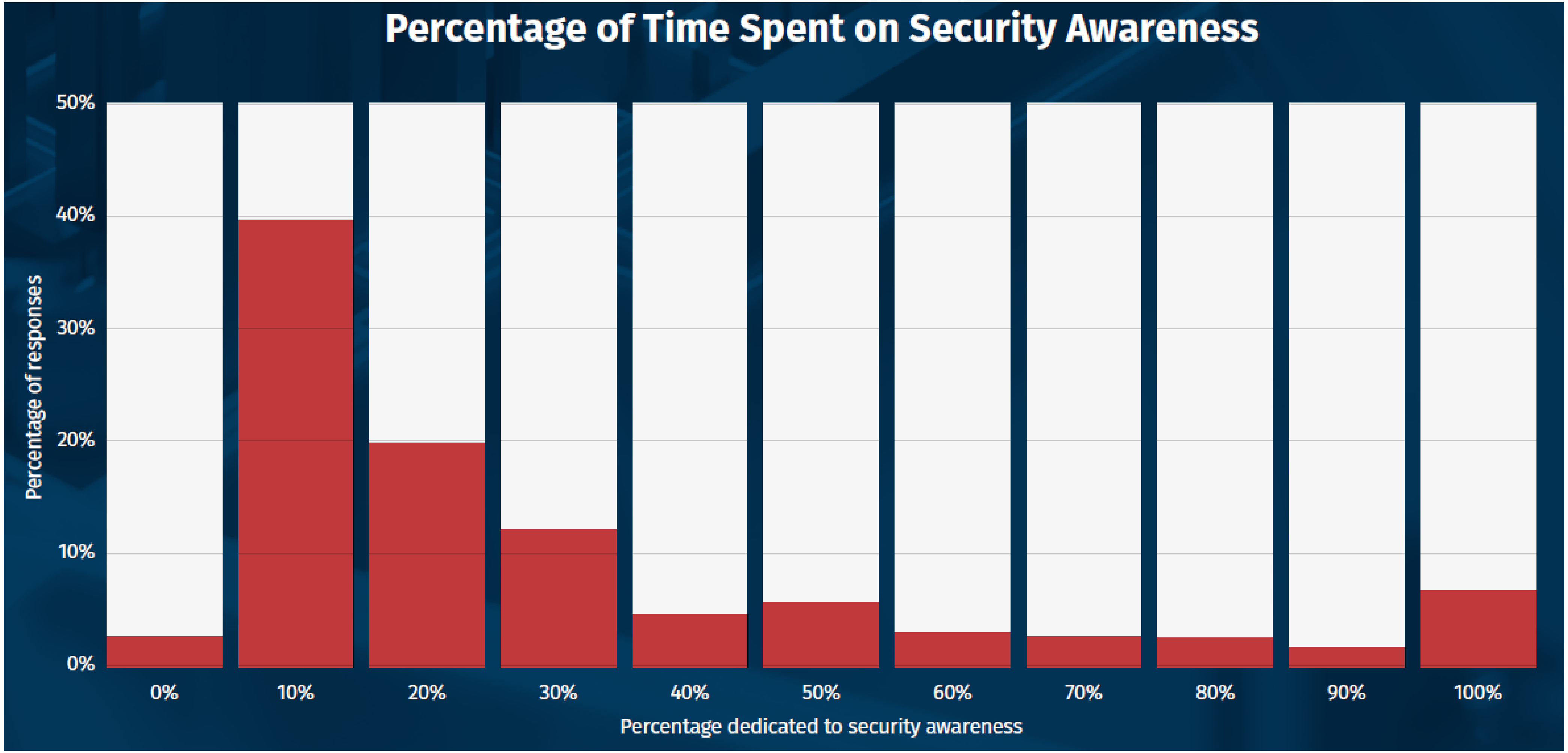
🟧 I have more support than I need



Top Reported Program Challenges

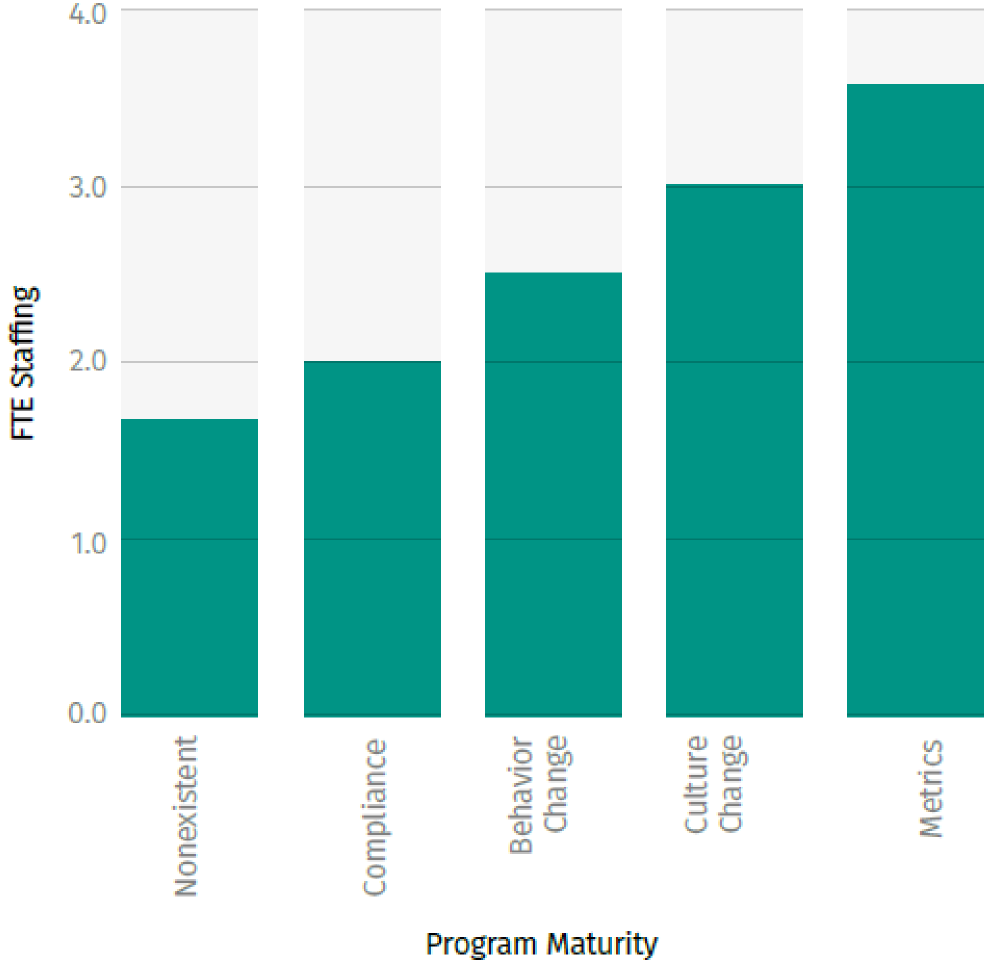


Over 80% of security awareness professionals reported that they spend half or less of their time on awareness, indicating far too often that security awareness is a part-time effort.

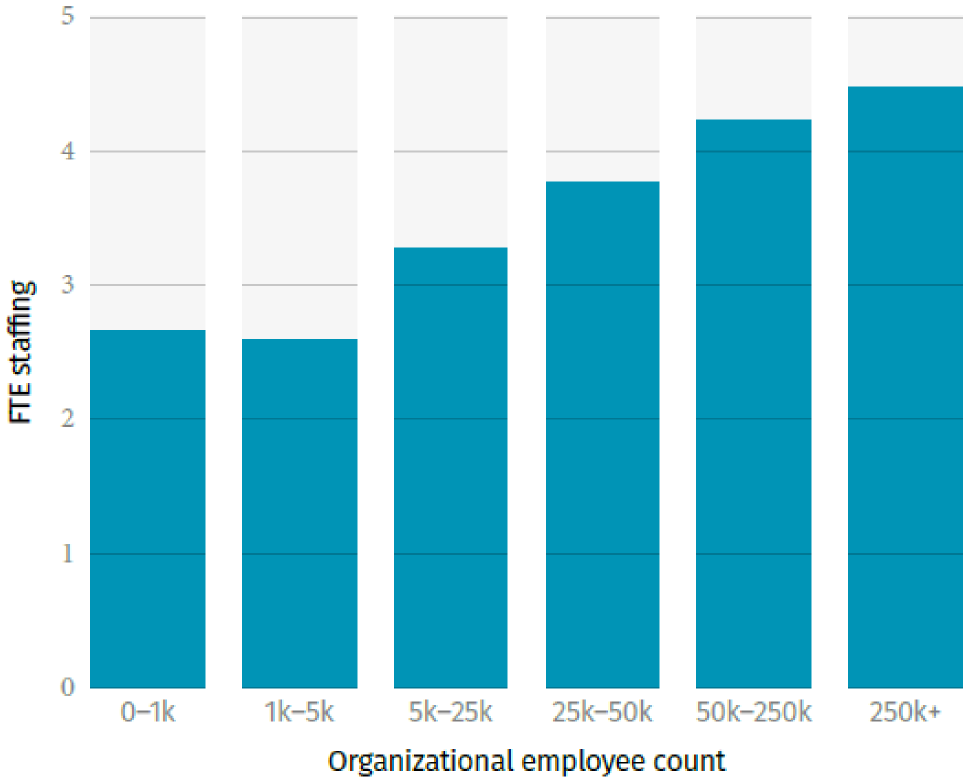


Percentage of Time Spent on Security Awareness

Average Number of FTEs by Maturity Level



Average Number of FTEs by Org Size

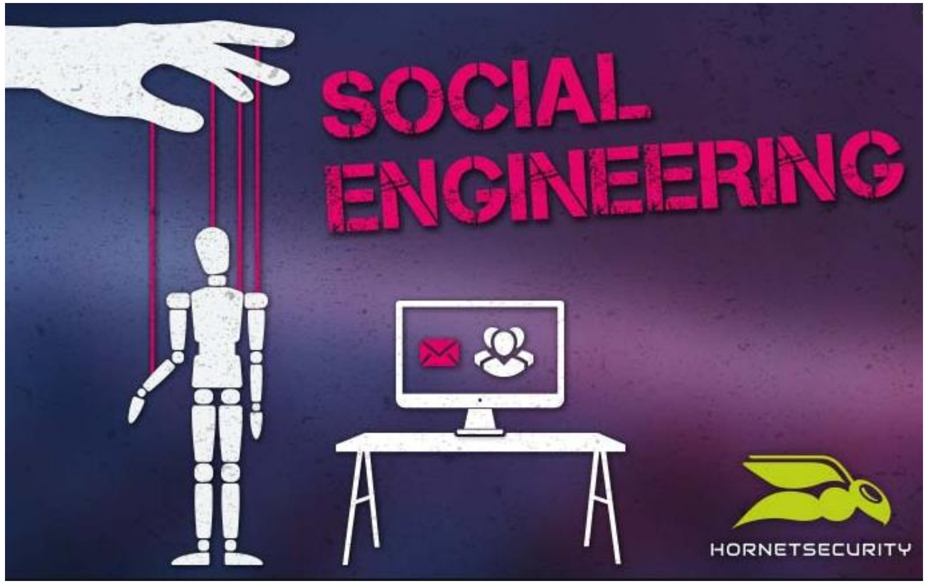


Agenda

- ✓Human element of cyber security
- ✓Employee risk
- ✓Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations’ Security Awareness and Training Programs
- Social Engineering

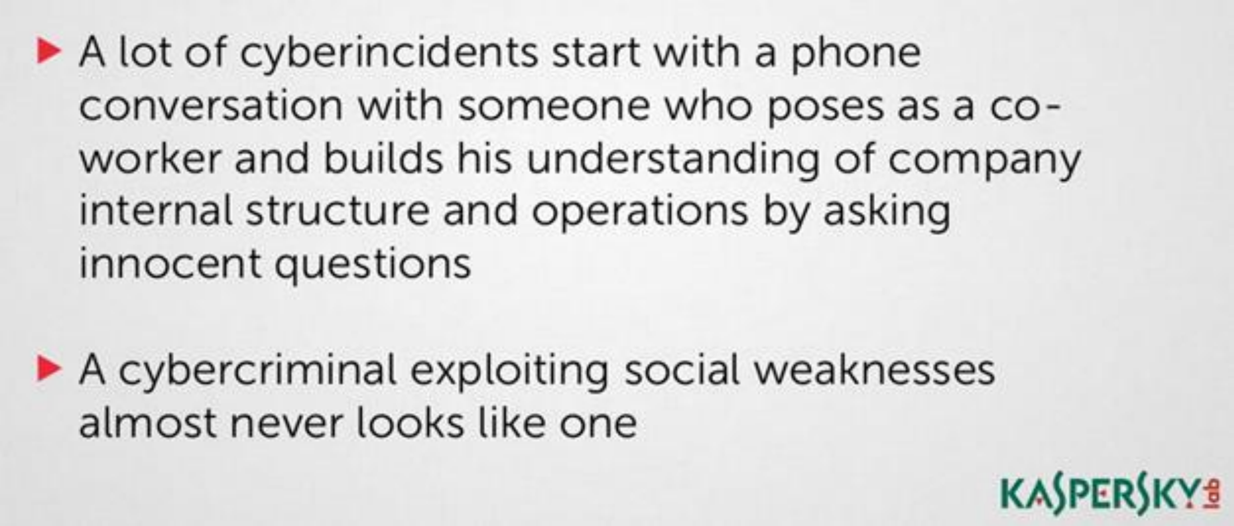
Creating a Security Aware Organization

An ongoing information security awareness program is vital - because of the need and importance of defending against social engineering and other information security threats



What is social engineering?

- Social engineering attacks have the same common element: deception (with the goal of getting an employee to do something the social engineer desires…)
  - Verify the identity of the person making an information request
  - Verify the person is authorized to receive the information



- A lot of cyberincidents start with a phone conversation with someone who poses as a co-worker and builds his understanding of company internal structure and operations by asking innocent questions
- A cybercriminal exploiting social weaknesses almost never looks like one

Common Social Engineering Strategies

- **Posing** as
  - a fellow employee
  - a new employee requesting help
  - someone in authority
  - a vendor or systems manufacturer calling to offer a system patch or update
  - an employee of a vendor, partner company, or law enforcement

- **Offering**…
  - help if a problem occurs, then making the problem occur, thereby manipulating the victim to call them for help
  - free software or patch for victim to install

Warning Signs of a Social Engineering Attack

- Refusal to give call back number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of non-compliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

Agenda

- ✓Human element of cyber security
- ✓Employee risk
- ✓Cyber Security Employee Awareness and Training Risk Controls
- ✓Evolution of Organizations’ Security Awareness and Training Programs
- ✓Social Engineering