Protecting Information Assets

- Unit# 3a -

Creating a Security Aware Organization

Agenda

- Awareness and Training Controls
- Creating a Security Aware Organization
  - Awareness and Training InfoSec Controls
  - The Threat landscape
  - Employee risk
  - Training course content (examples)
- Test Taking Tip
- Quiz

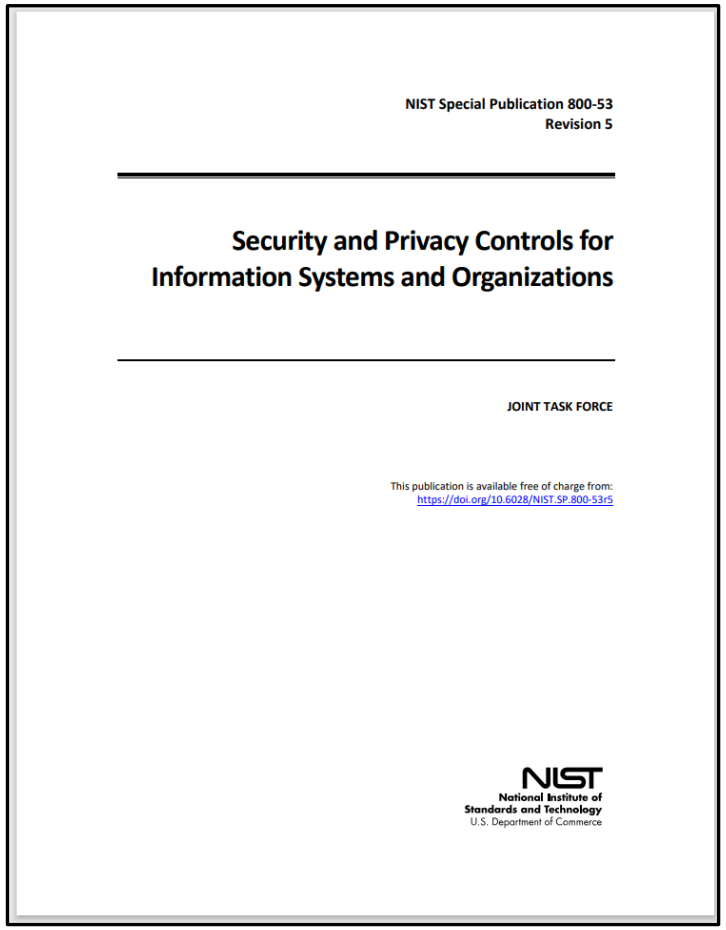


TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

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

Note: NIST SP 800-53x InfoSec control documents can be found on the MIS Community Site, in the WrapUp post for this Unit 3a

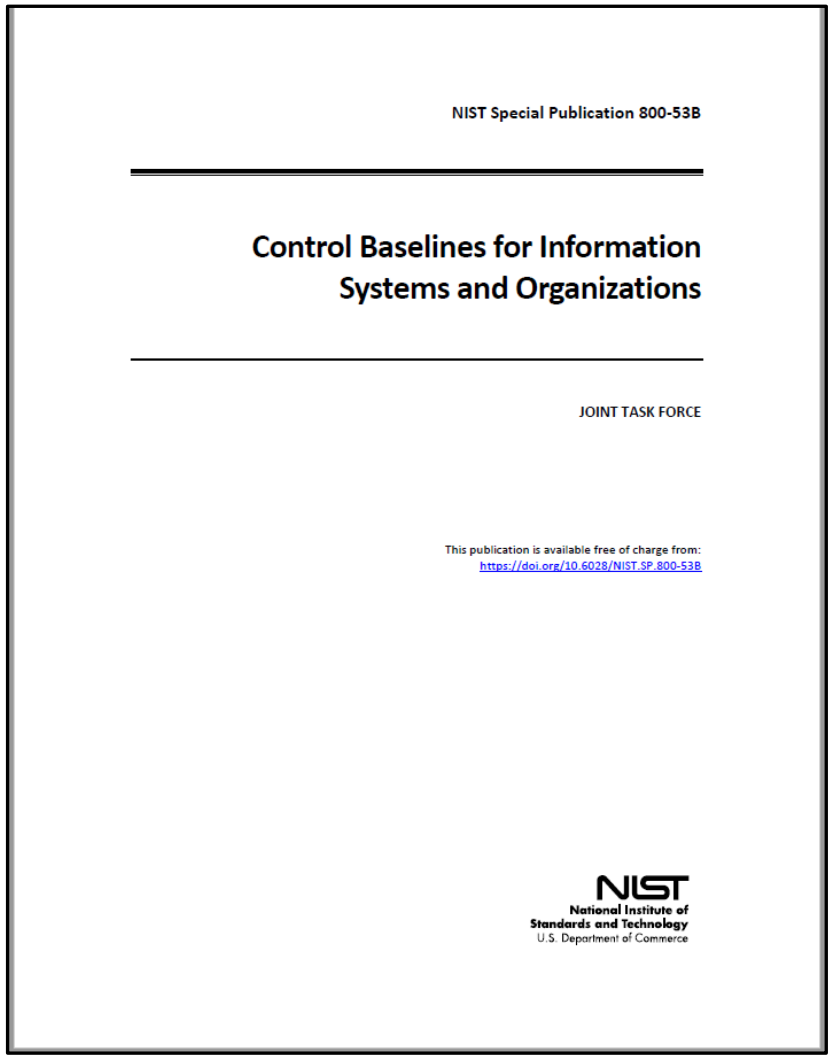


TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	X	X	X	X
AT-2	**Literacy Training and Awareness**	X	X	X	X
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			X	X
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	X	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	X			
AT-4	**Training Records**	X	X	X	X
AT-5	**Contacts with Security Groups and Associations**	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	x	x	x	x
AT-2	**Literacy Training and Awareness**	x	x	x	x
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	x	x	x	x
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4)			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	x			
AT-4	**Training Records**	x	x	x	x
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

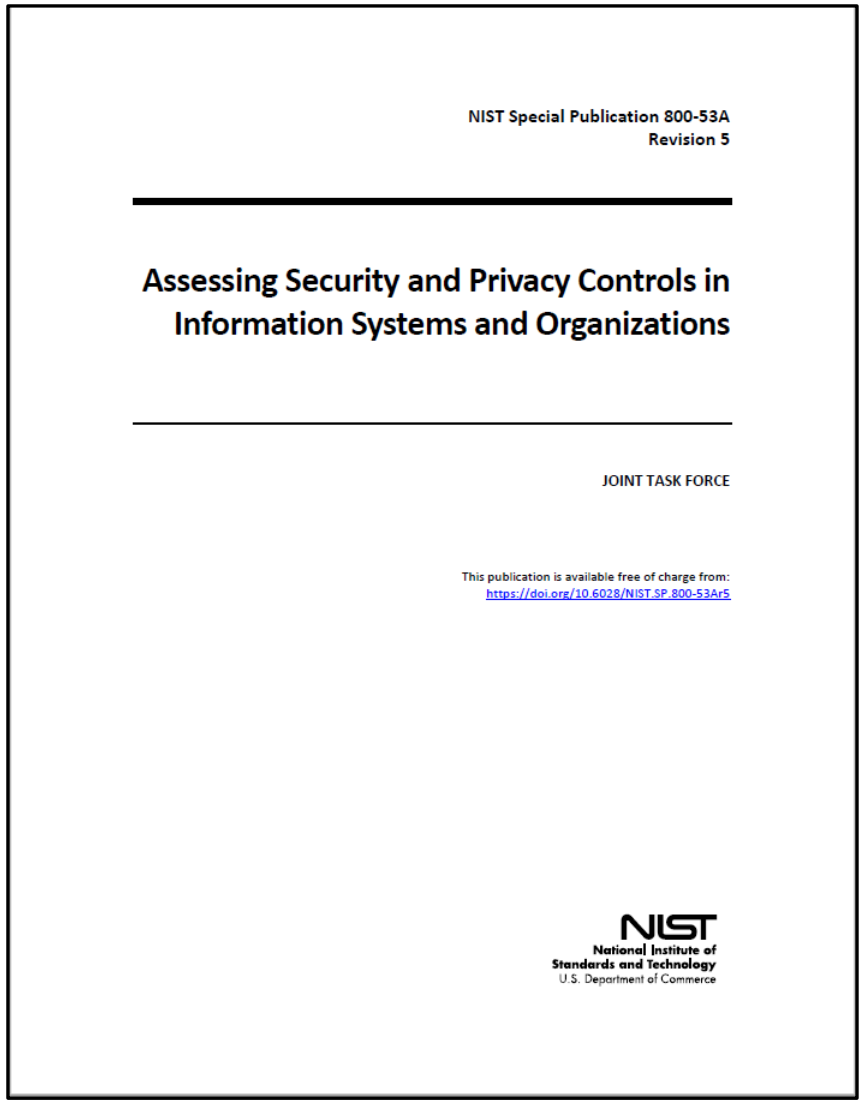
Remember the Disaster Management Information Systems…

Determination of overall security categorization…

Disaster Management Information Systems

Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	*High*
Disaster Preparedness and Planning	Low	Low	Low	*Low*
Disaster Repair and Restoration	Low	Low	Low	*Low*
Emergency Response Information Type	Low	High	High	*High*
Information System Impact Ratings:	Low	High	High	*High*

How would you audit these risk controls?



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

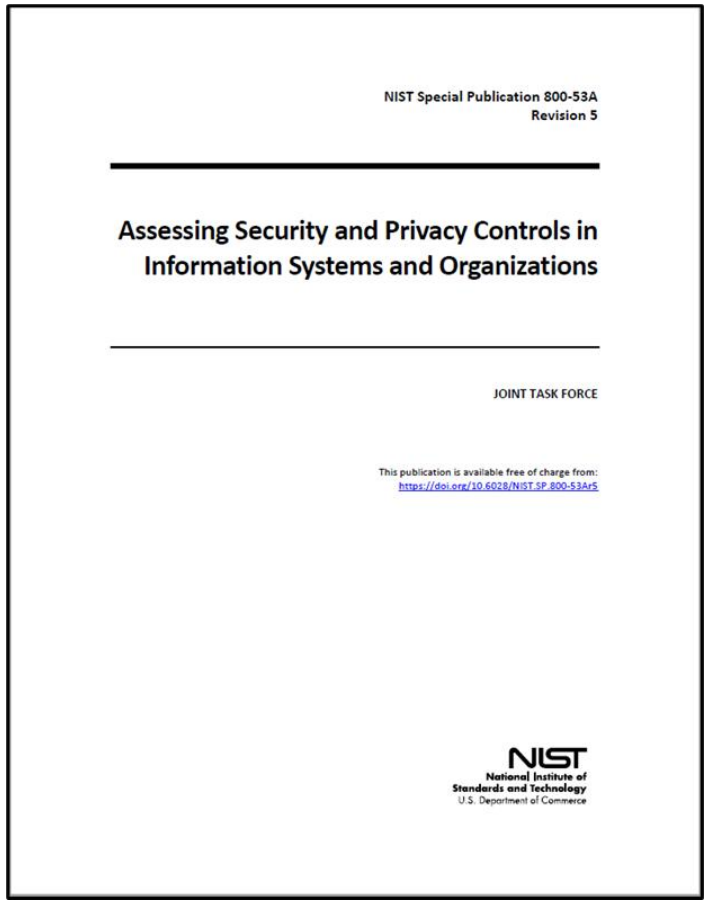
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	X	X	X	X
AT-2	**Literacy Training and Awareness**	X	X	X	X
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			X	X
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	X	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	X			
AT-4	**Training Records**	X	X	X	X
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

Exercise:

- ***Find an audit control checklist for AT-1…***



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

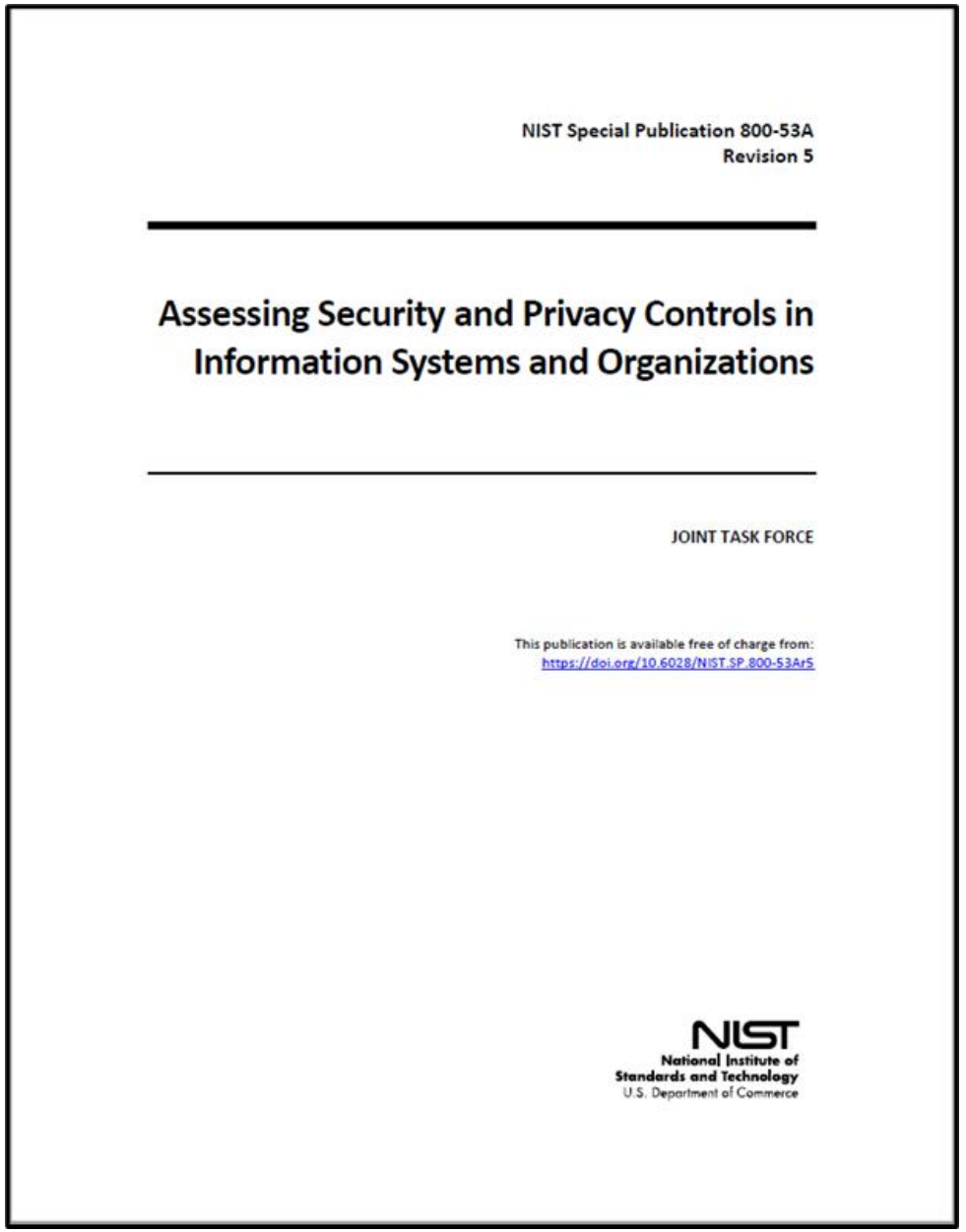
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

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

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	X	X	X	X
AT-2	**Literacy Training and Awareness**	X	X	X	X
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			X	X
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	X	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	X			
AT-4	**Training Records**	X	X	X	X
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

AT-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-01_ODP[01]	***personnel or roles to whom the awareness and training policy is to be disseminated is/are defined;***
	AT-01_ODP[02]	***personnel or roles to whom the awareness and training procedures are to be disseminated is/are defined;***
	AT-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	AT-01_ODP[04]	***an official to manage the awareness and training policy and procedures is defined;***
	AT-01_ODP[05]	***the frequency at which the current awareness and training policy is reviewed and updated is defined;***
	AT-01_ODP[06]	***events that would require the current awareness and training policy to be reviewed and updated are defined;***
	AT-01_ODP[07]	***the frequency at which the current awareness and training procedures are reviewed and updated is defined;***
	AT-01_ODP[08]	***events that would require procedures to be reviewed and updated are defined;***
	AT-01a.[01]	an awareness and training policy is developed and documented;
	AT-01a.[02]	the awareness and training policy is disseminated to ***<AT-01_ODP[01] personnel or roles>***;
	AT-01a.[03]	awareness and training procedures to facilitate the implementation of the awareness and training policy and associated access controls are developed and documented;
	AT-01a.[04]	the awareness and training procedures are disseminated to ***<AT-01_ODP[02] personnel or roles>***.
	AT-01a.01(a)[01]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses purpose;
	AT-01a.01(a)[02]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses scope;
	AT-01a.01(a)[03]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses roles;
	AT-01a.01(a)[04]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses responsibilities;
	AT-01a.01(a)[05]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses management commitment;
	AT-01a.01(a)[06]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses coordination among organizational entities;
	AT-01a.01(a)[07]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses compliance; and



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

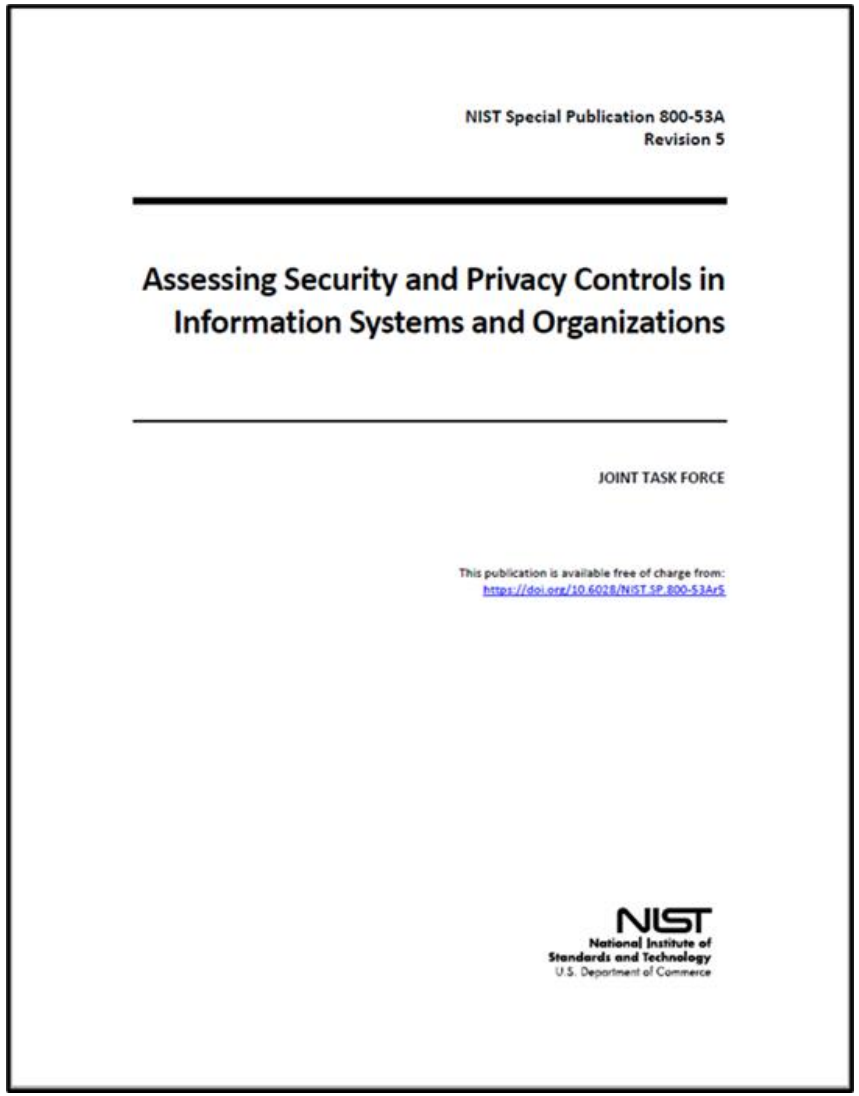
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

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

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	X	X	X	X
AT-2	**Literacy Training and Awareness**	X	X	X	X
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			X	X
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	X	X	X	X
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	X			
AT-4	**Training Records**	X	X	X	X
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

How would you assess the training?



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

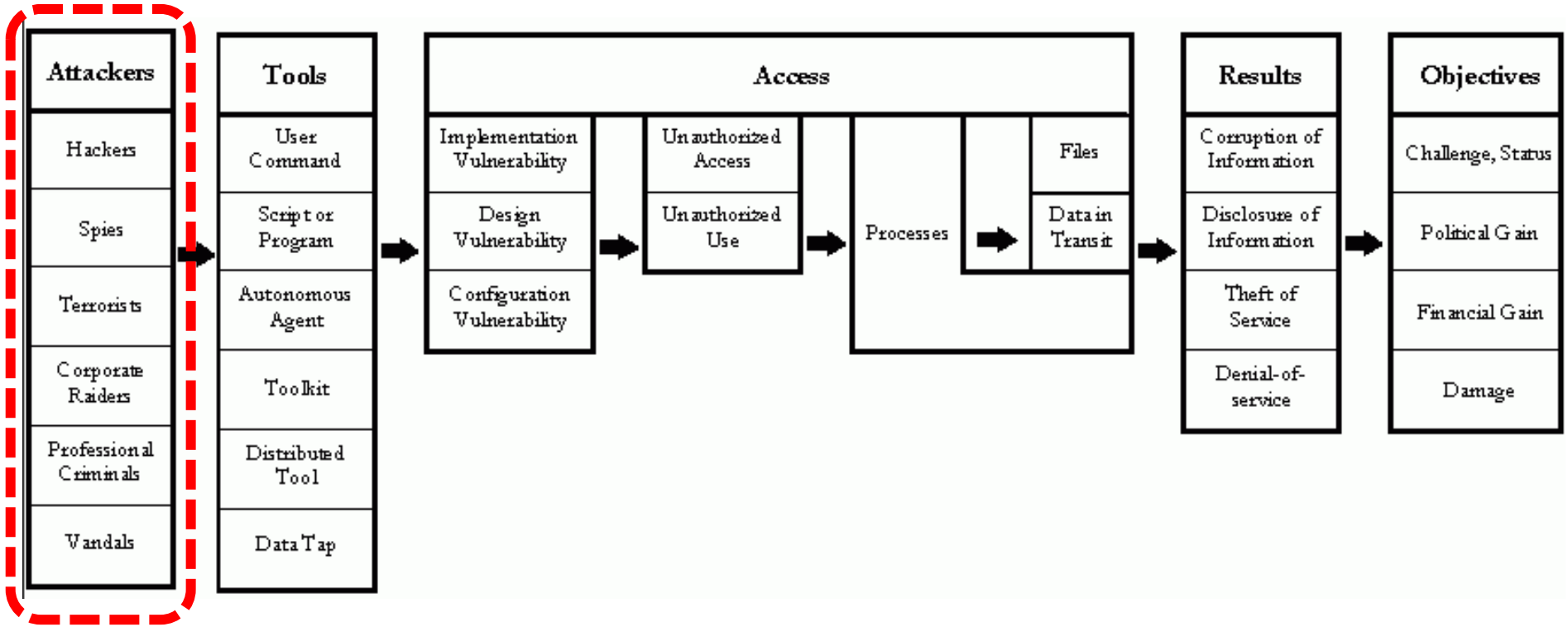
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

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

AT-02	LITERACY TRAINING AND AWARENESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02_ODP[01]	***the frequency at which to provide security literacy training to system users (including managers, senior executives, and contractors) after initial training is defined;***
	AT-02_ODP[02]	***the frequency at which to provide privacy literacy training to system users (including managers, senior executives, and contractors) after initial training is defined;***
	AT-02_ODP[03]	***events that require security literacy training for system users are defined;***
	AT-02_ODP[04]	***events that require privacy literacy training for system users are defined;***
	AT-02_ODP[05]	***techniques to be employed to increase the security and privacy awareness of system users are defined;***
	AT-02_ODP[06]	***the frequency at which to update literacy training and awareness content is defined;***
	AT-02_ODP[07]	***events that would require literacy training and awareness content to be updated are defined;***
	AT-02a.01[01]	security literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users;

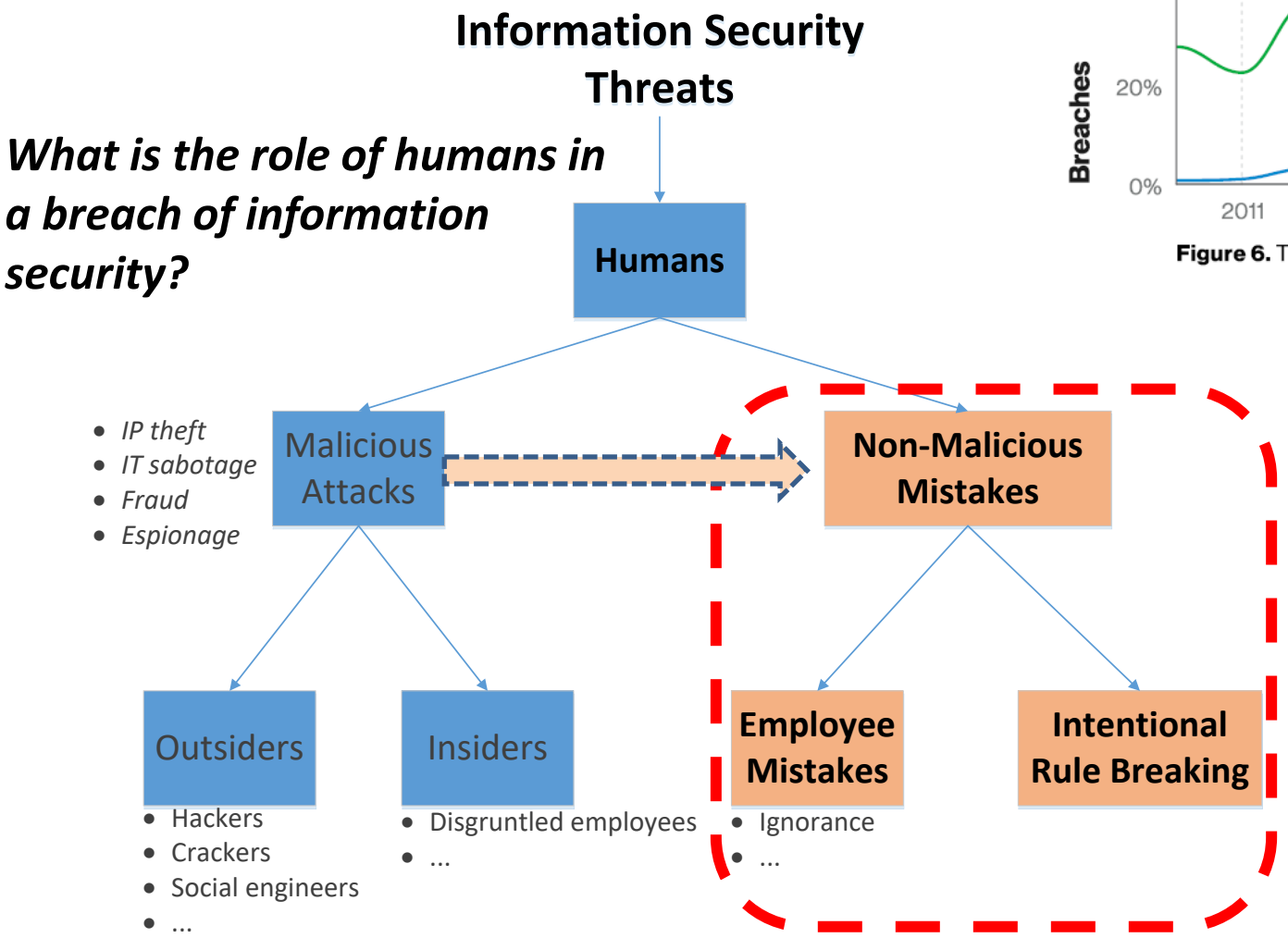
AT-02	LITERACY TRAINING AND AWARENESS	
	AT-02a.01[02]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users;
	AT-02a.01[03]	security literacy training is provided to system users (including managers, senior executives, and contractors) ***<AT-02_ODP[01] frequency>*** thereafter;
	AT-02a.01[04]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) ***<AT-02_ODP[02] frequency>*** thereafter;
	AT-02a.02[01]	security literacy training is provided to system users (including managers, senior executives, and contractors) when required by system changes or following ***<AT-02_ODP[03] events>***;
	AT-02a.02[02]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) when required by system changes or following ***<AT-02_ODP[04] events>***;
	AT-02b.	***<AT-02_ODP[05] awareness techniques>*** are employed to increase the security and privacy awareness of system users;
	AT-02c.[01]	literacy training and awareness content is updated ***<AT-02_ODP[06] frequency>***;
	AT-02c.[02]	literacy training and awareness content is updated following ***<AT-02_ODP[07] events>***;
	AT-02d.	lessons learned from internal or external security incidents or breaches are incorporated into literacy training and awareness techniques.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; appropriate codes of federal regulations; security and privacy literacy training curriculum; security and privacy literacy training materials; training records; other relevant documents or records].
	AT-02-Interview	[SELECT FROM: Organizational personnel with responsibilities for literacy training and awareness; organizational personnel with information security and privacy responsibilities; organizational personnel comprising the general system user community].
	AT-02-Test	[SELECT FROM: Mechanisms managing information security and privacy literacy training].

What is in this picture ?
What is missing from this diagram?



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….



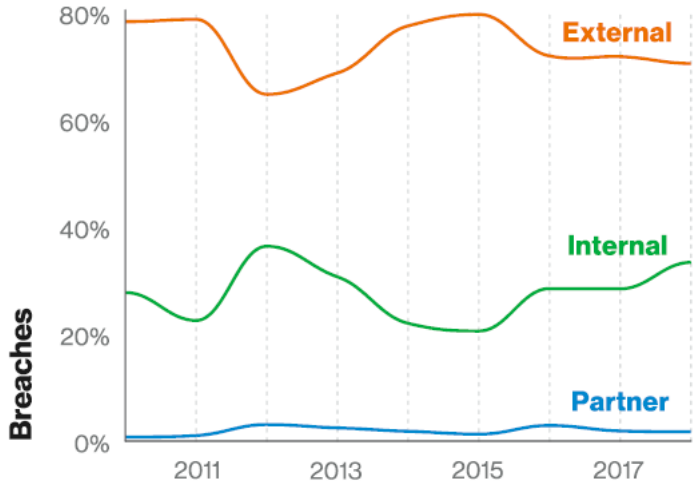


Figure 6. Threat actors in breaches over time

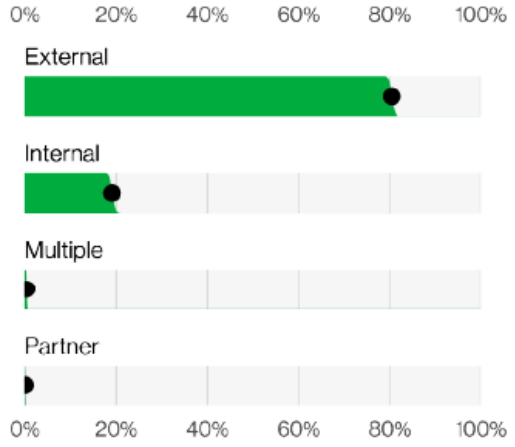
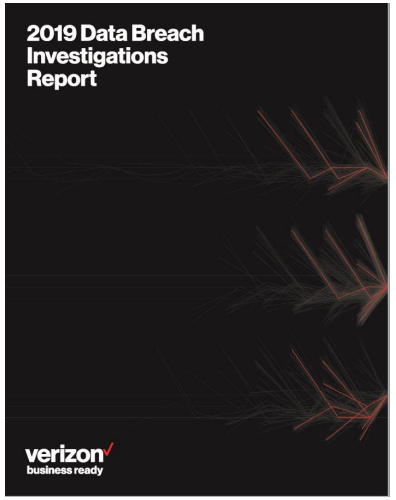
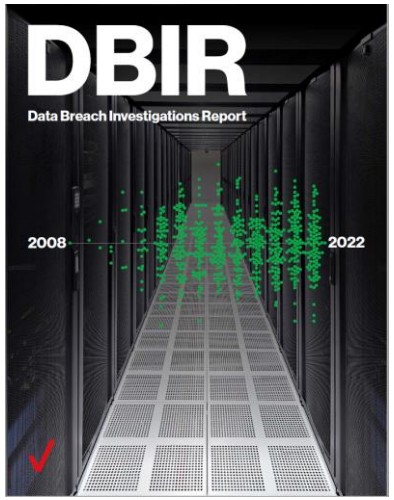


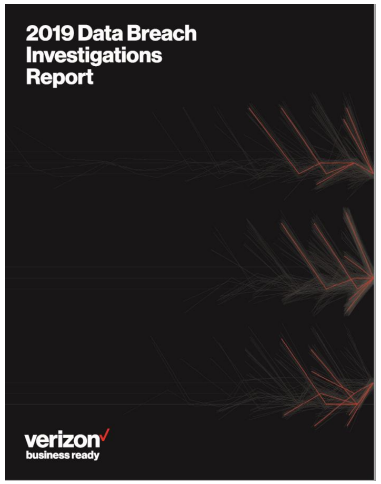
Figure 11. Actors in breaches (n=5,146)





https://www.verizon.com/business/resources/reports/dbir

What roles do employees play in these attack chains



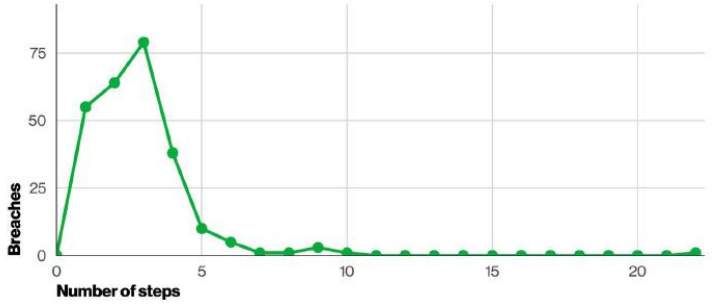


Figure 30. Number of steps per breach in non-Error breaches (n=258)

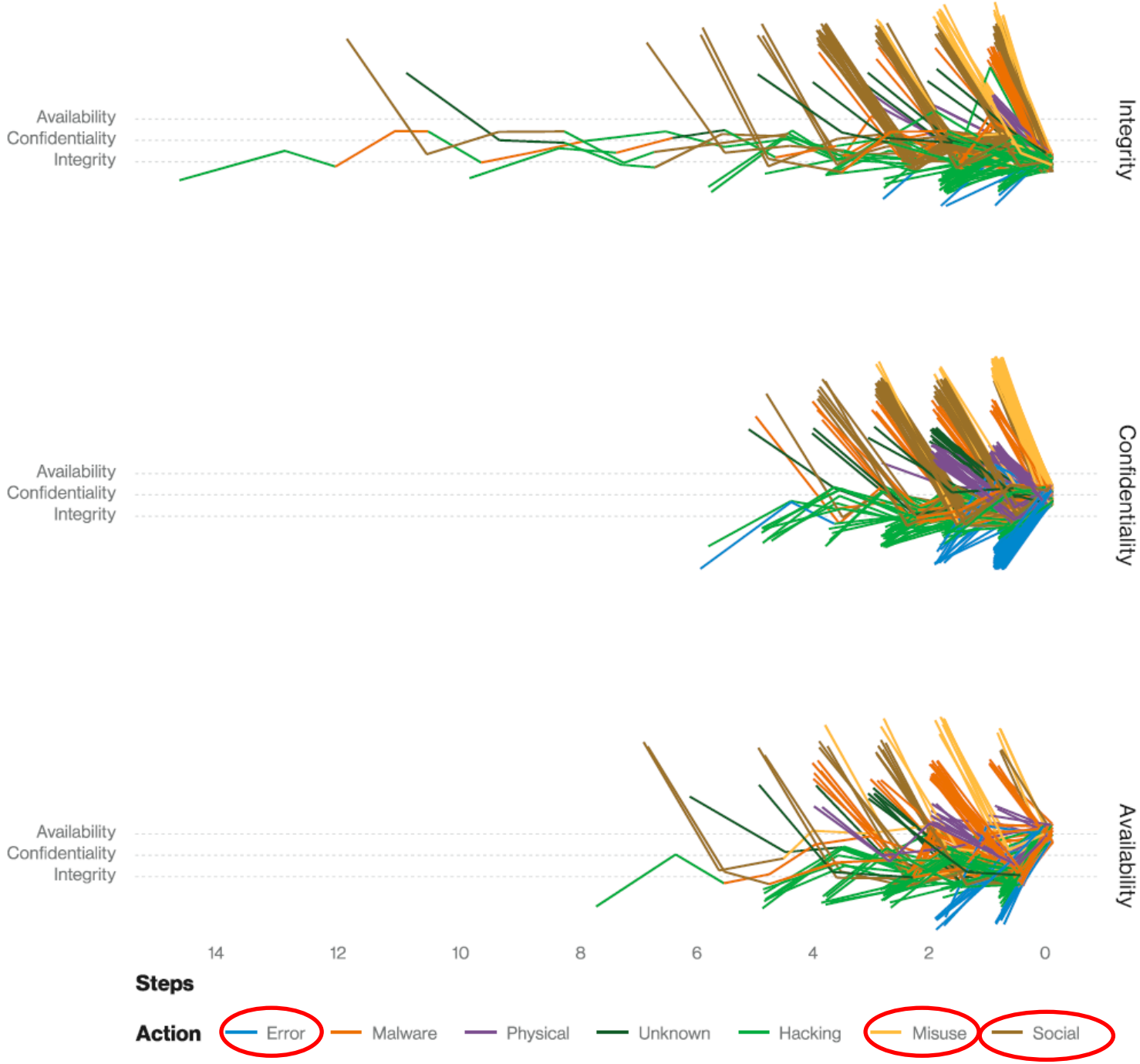


Figure 30. Attack chain by final attribute compromised[12] (n=941)

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?

Patterns in breaches

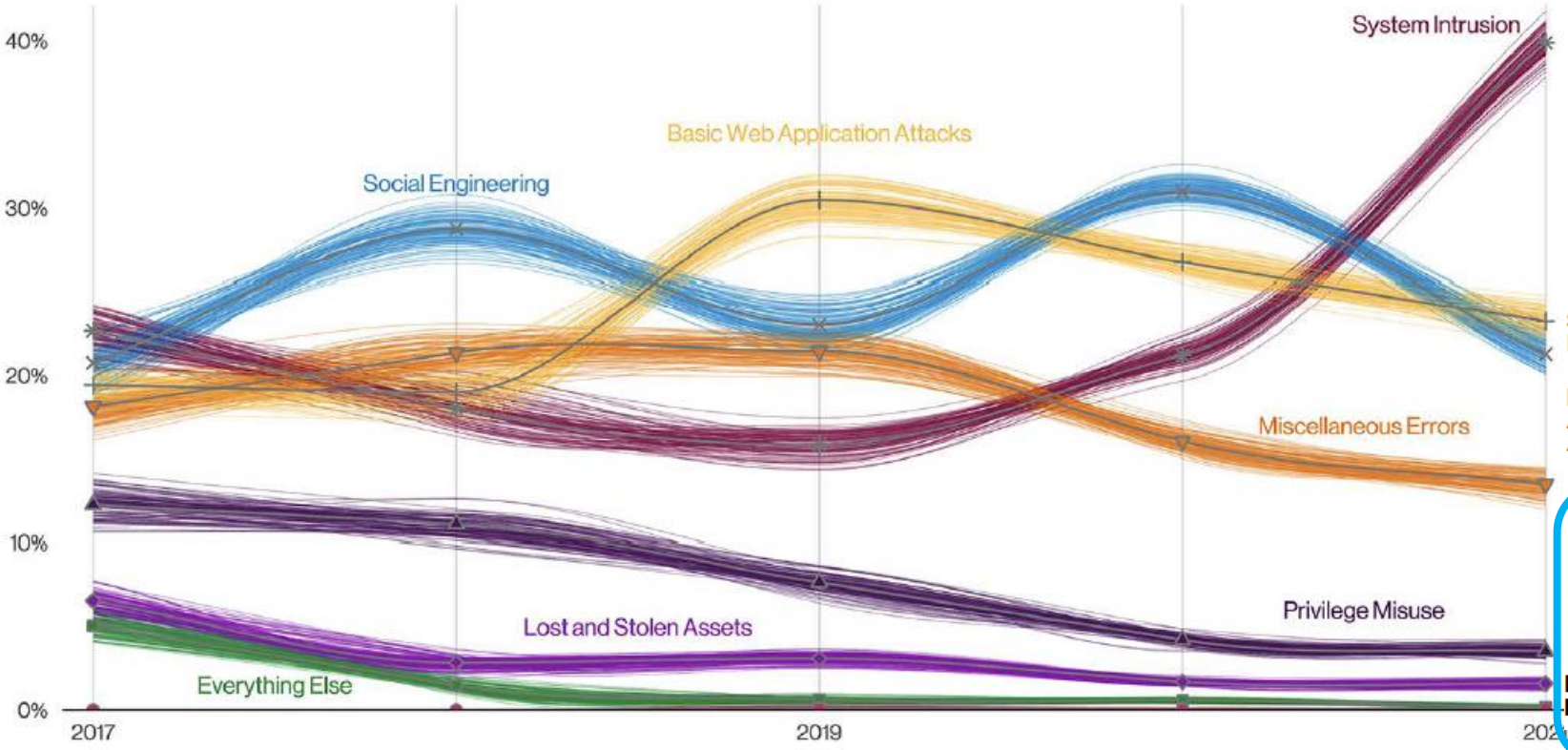


Figure 33. Patterns over time in breaches

System Intrusion	Complex attacks that leverage malware and/or hacking to achieve their objectives including deploying Ransomware.
Basic Web Application Attacks	These attacks are against a Web application, and after initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.
Social Engineering	A psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges.

Employee risk areas…

Employee Risk

Firewall and email filters to weed out phishing emails and malicious websites are important, but they're not enough

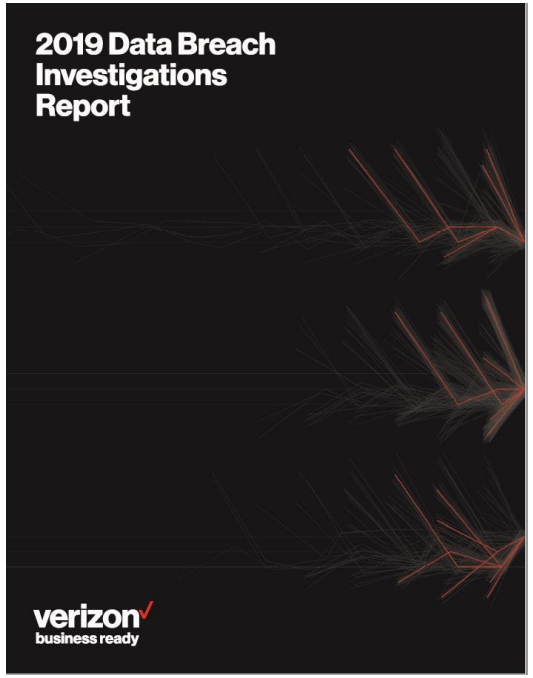
- Organizations must also ensure their security posture is good by:
  - Setting policies, educating staff, and enforcing good security hygiene
  - Taking advantage of the security options that are available
  - Training and testing employees
  - Implementing automated checks to ensure their security posture

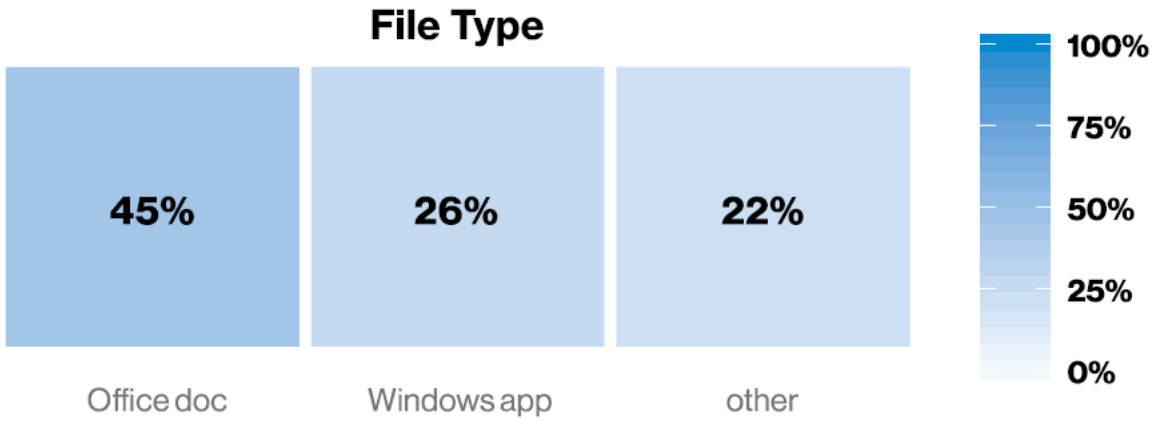
Employee Risk

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





Over 40% of breaches used stolen credentials

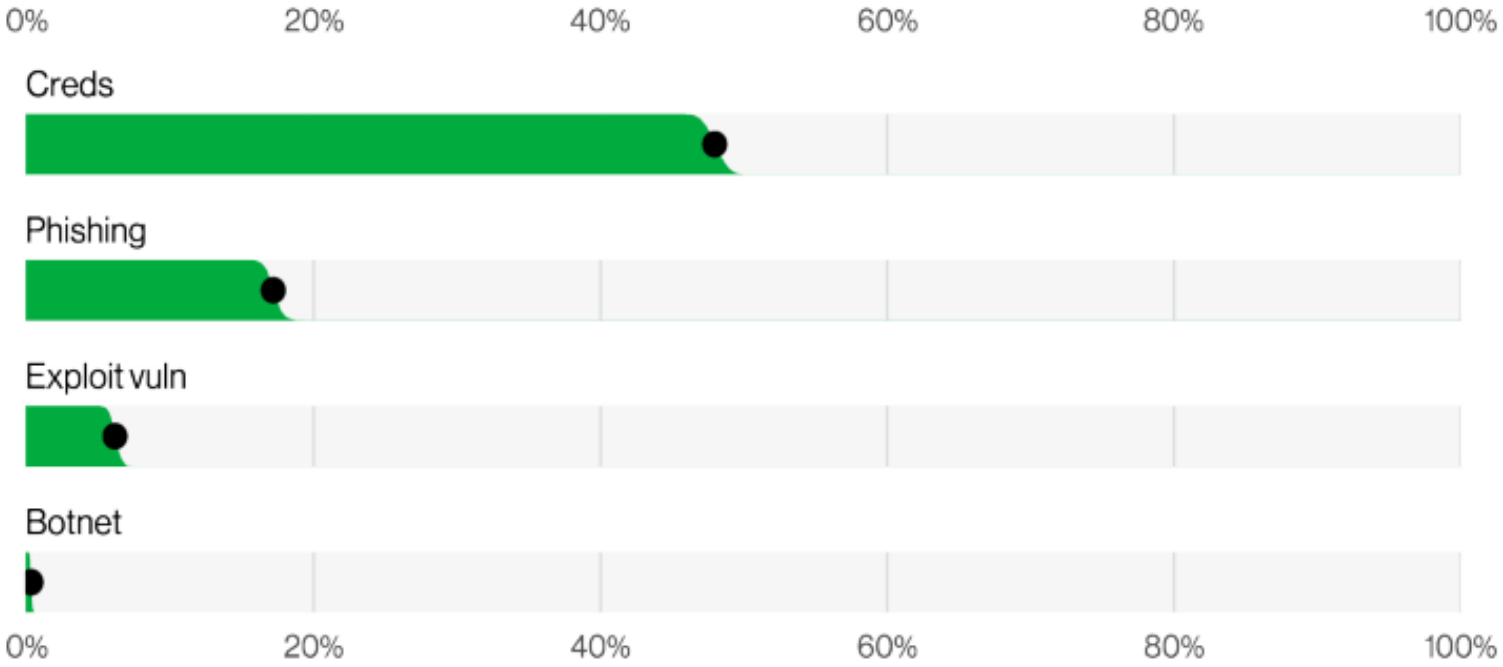


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

Ponemon INSTITUTE

October 2020

Cybersecurity in the Remote Work Era:

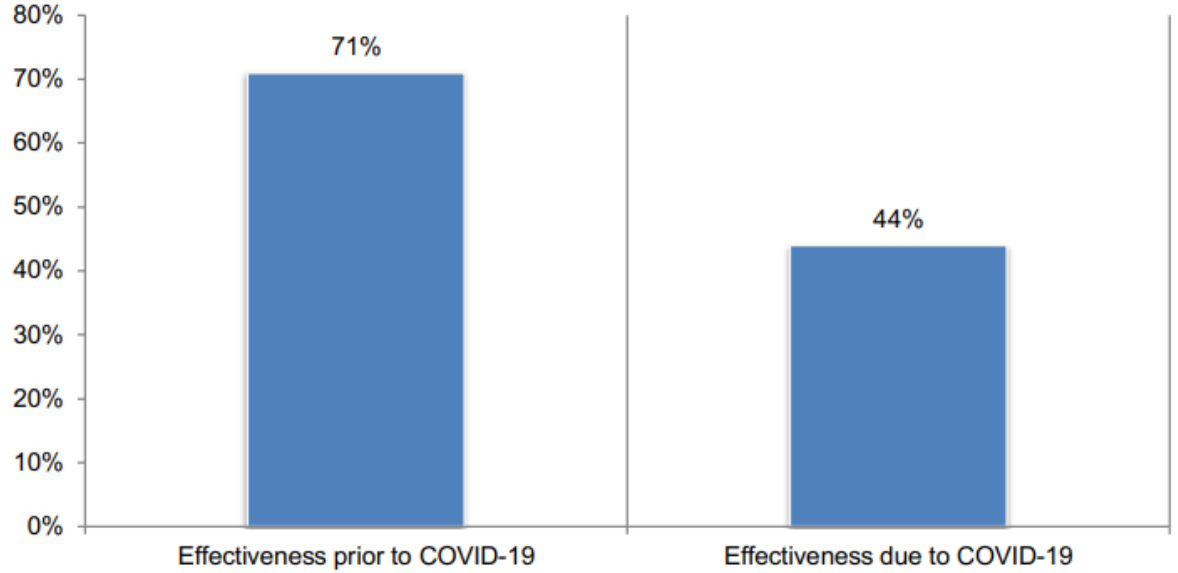
A Global Risk Report

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

KEEPER Cybersecurity Starts Here

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



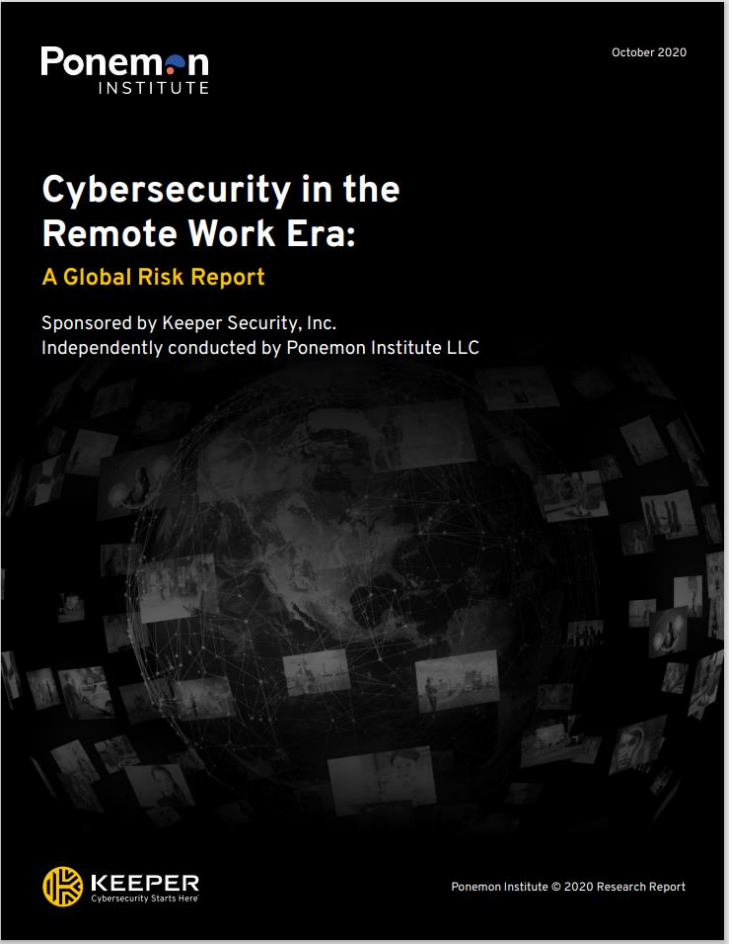
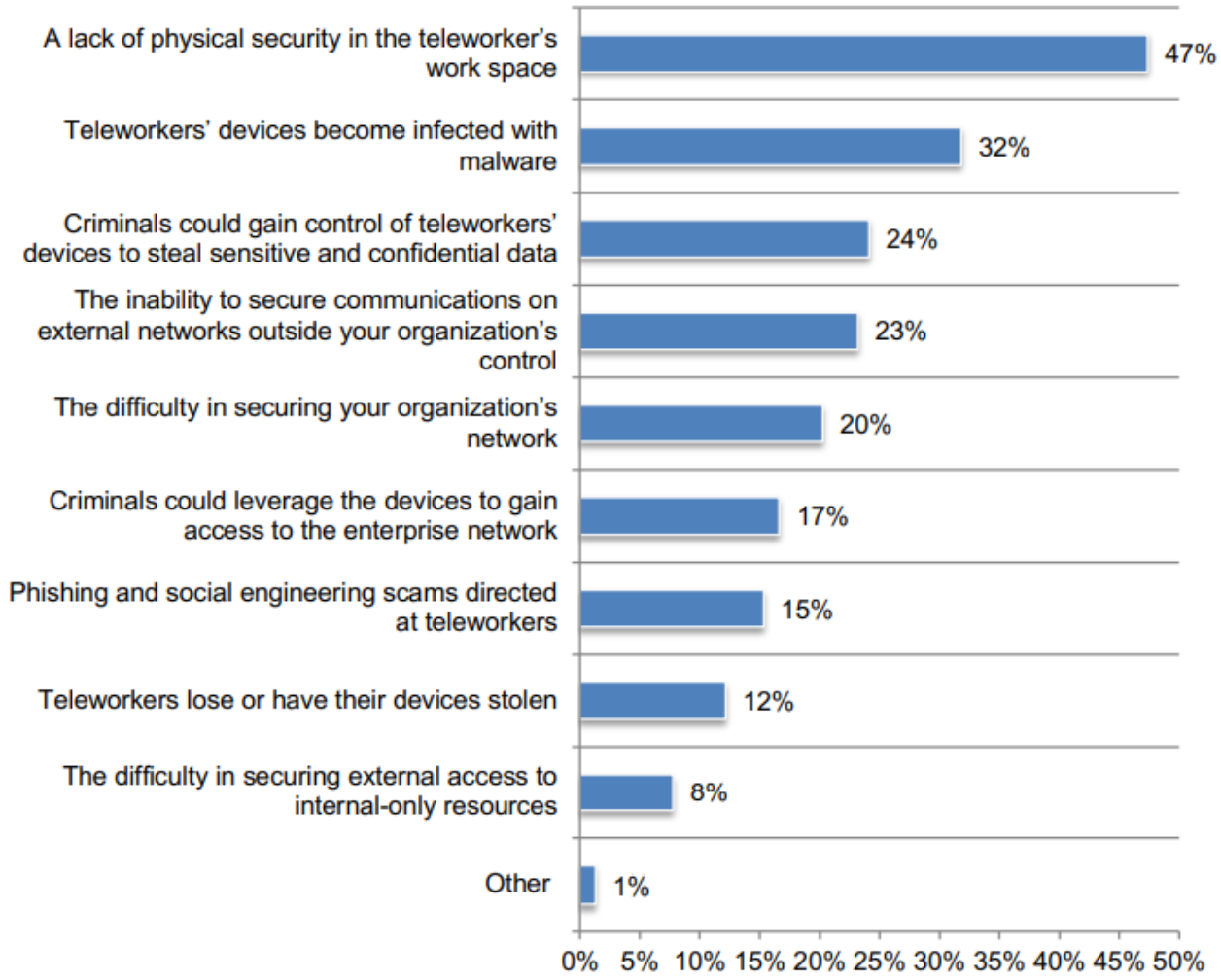


Figure 3. Security risks organizations are most concerned about
More than one response permitted



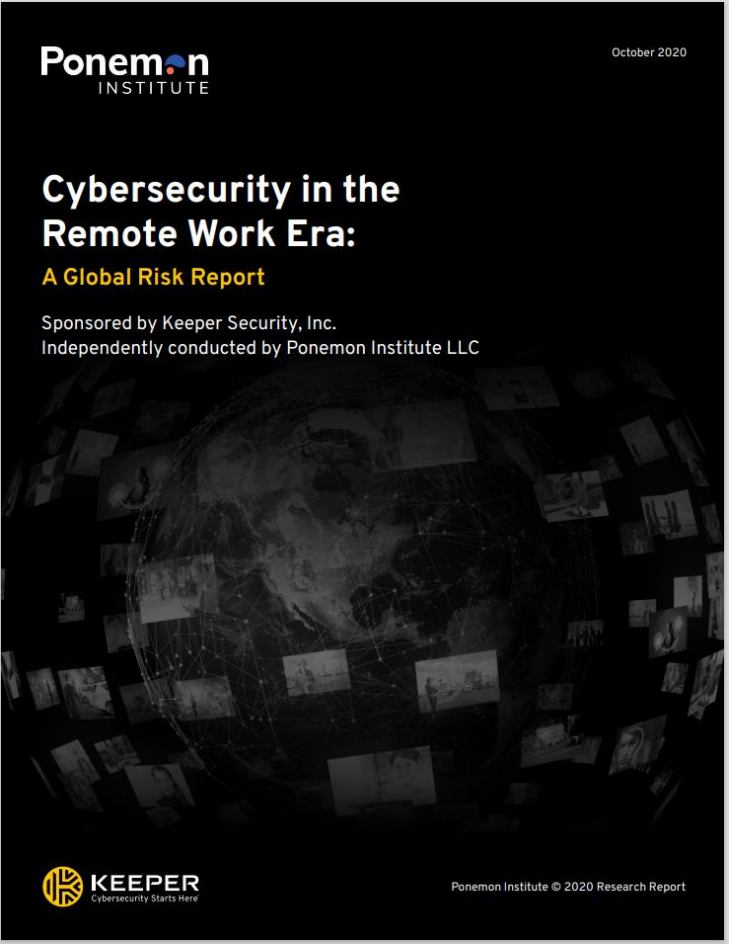
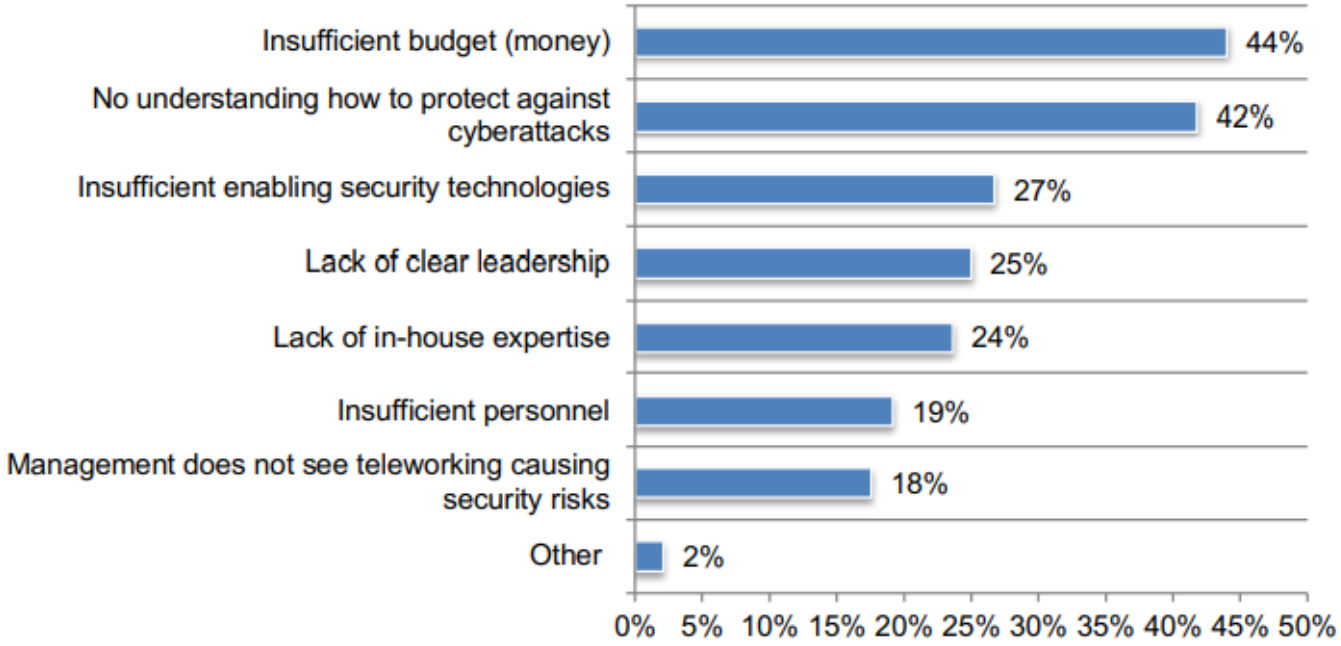


Figure 5. What challenges keep your organization's IT security posture from being fully effective due to teleworking?
Two responses permitted



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…

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

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…"

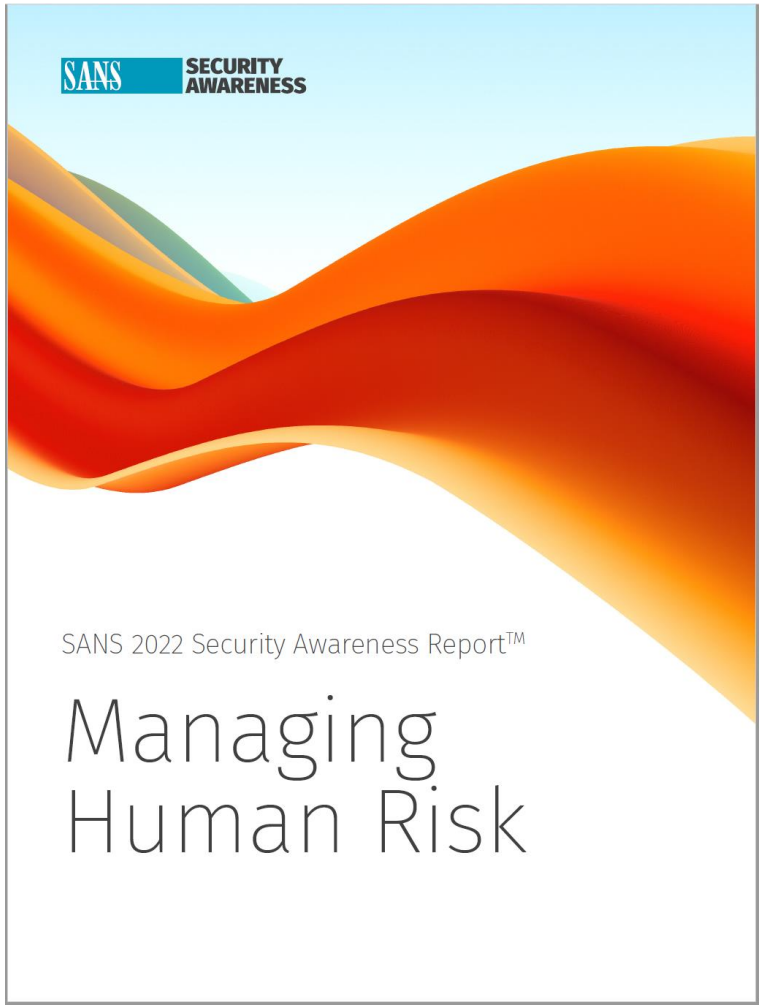
Auditing a Security Awareness Training control enhancement

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].

TABLE 3-2: AWARENESS AND TRAINING FAMILY

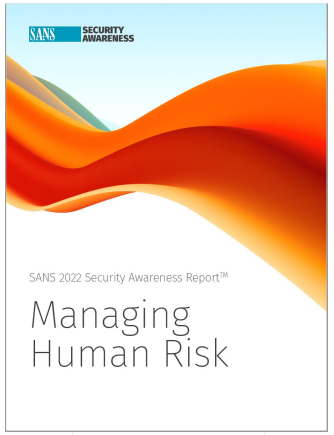
CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	x	x	x	x
AT-2	**Literacy Training and Awareness**	x	x	x	x
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-Based Training**	x	x	x	x
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	x			
AT-4	**Training Records**	x	x	x	x
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

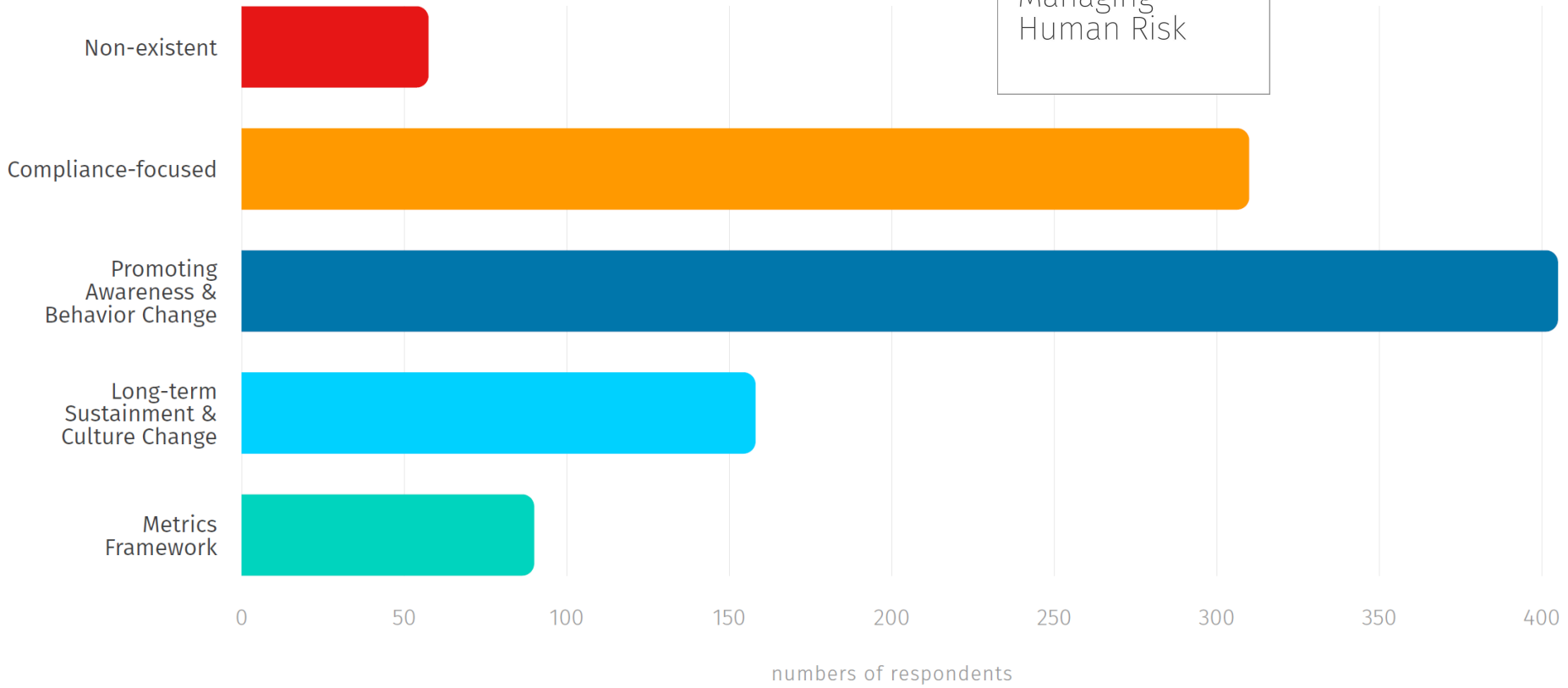
What phases of security awareness do organizations go through as their programs mature?

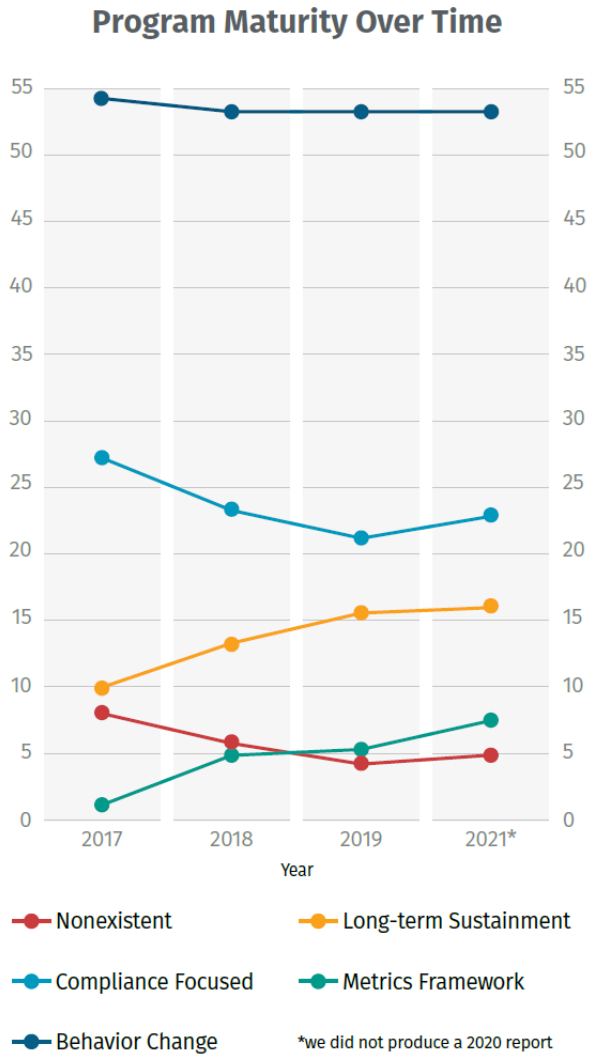


https://www.sans.org/blog/sans-2022-security-awareness-report/

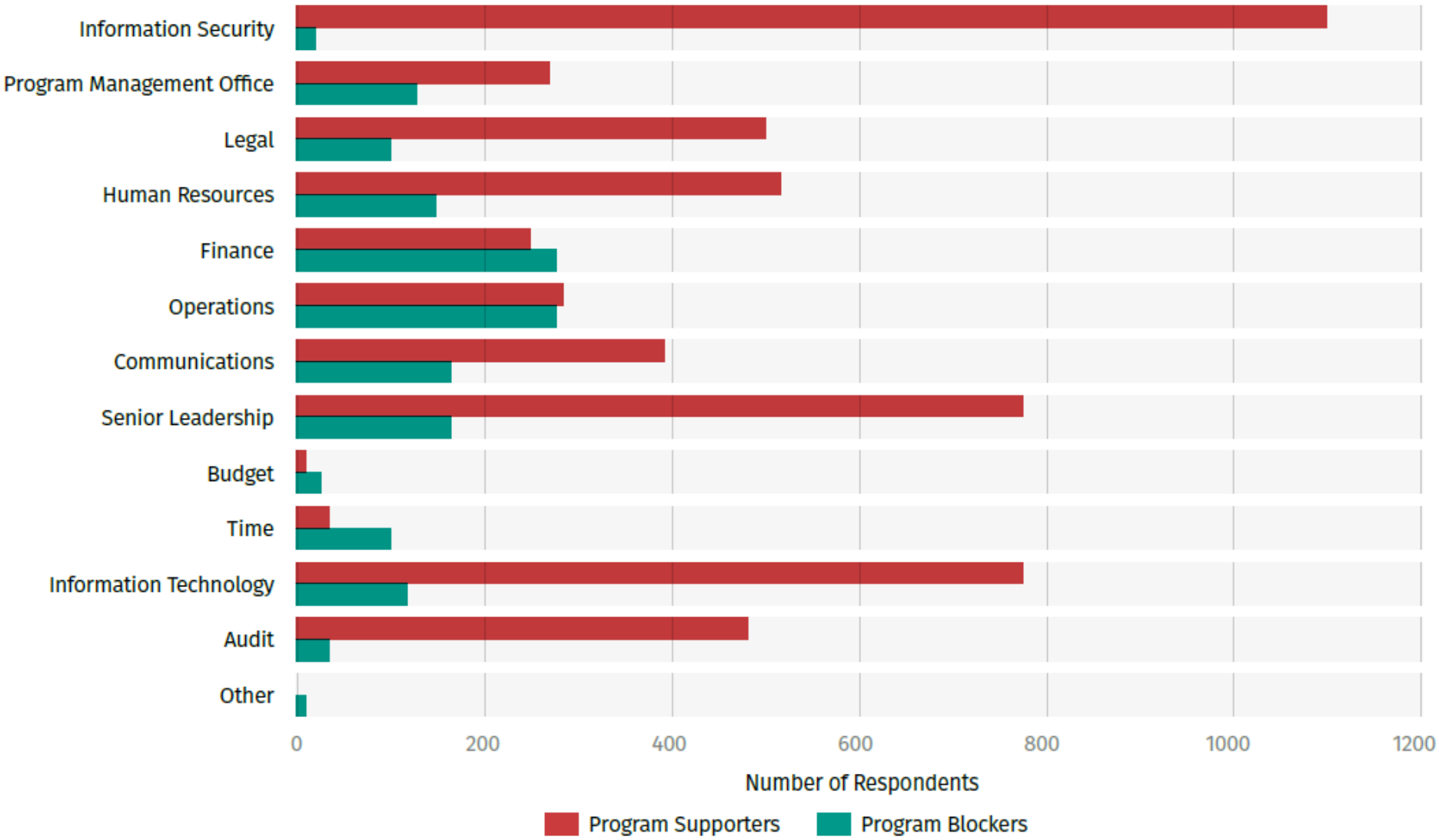

2021 SECURITY AWARENESS REPORT™
MANAGING
HUMAN CYBER
RISK

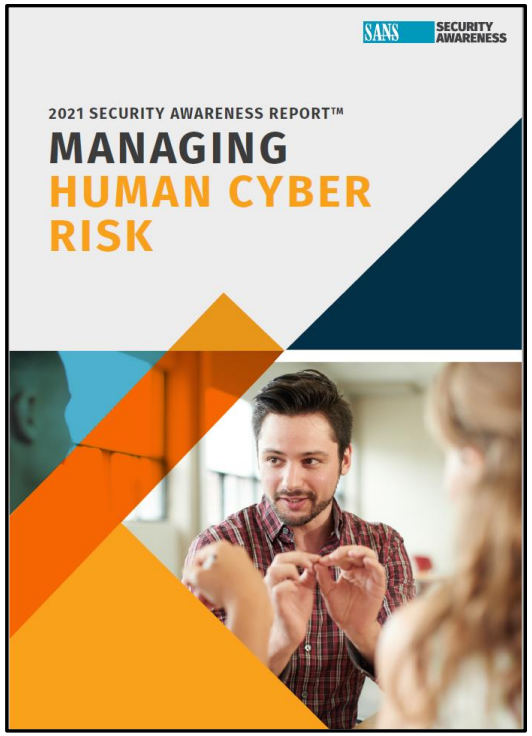

SANS SECURITY AWARENESS
SANS 2022 Security Awareness Report™
Managing
Human Risk


Current Maturity Level
Non-existent
Compliance-focused
Promoting Awareness & Behavior Change
Long-term Sustainment & Culture Change
Metrics Framework
0
50
100
150
200
250
300
350
400
numbers of respondents


Program Maturity Over Time
55
50
45
40
35
30
25
20
15
10
5
0
2017
2018
2019
2021*
Year
Nonexistent
Long-term Sustainment
Compliance Focused
Metrics Framework
Behavior Change
*we did not produce a 2020 report

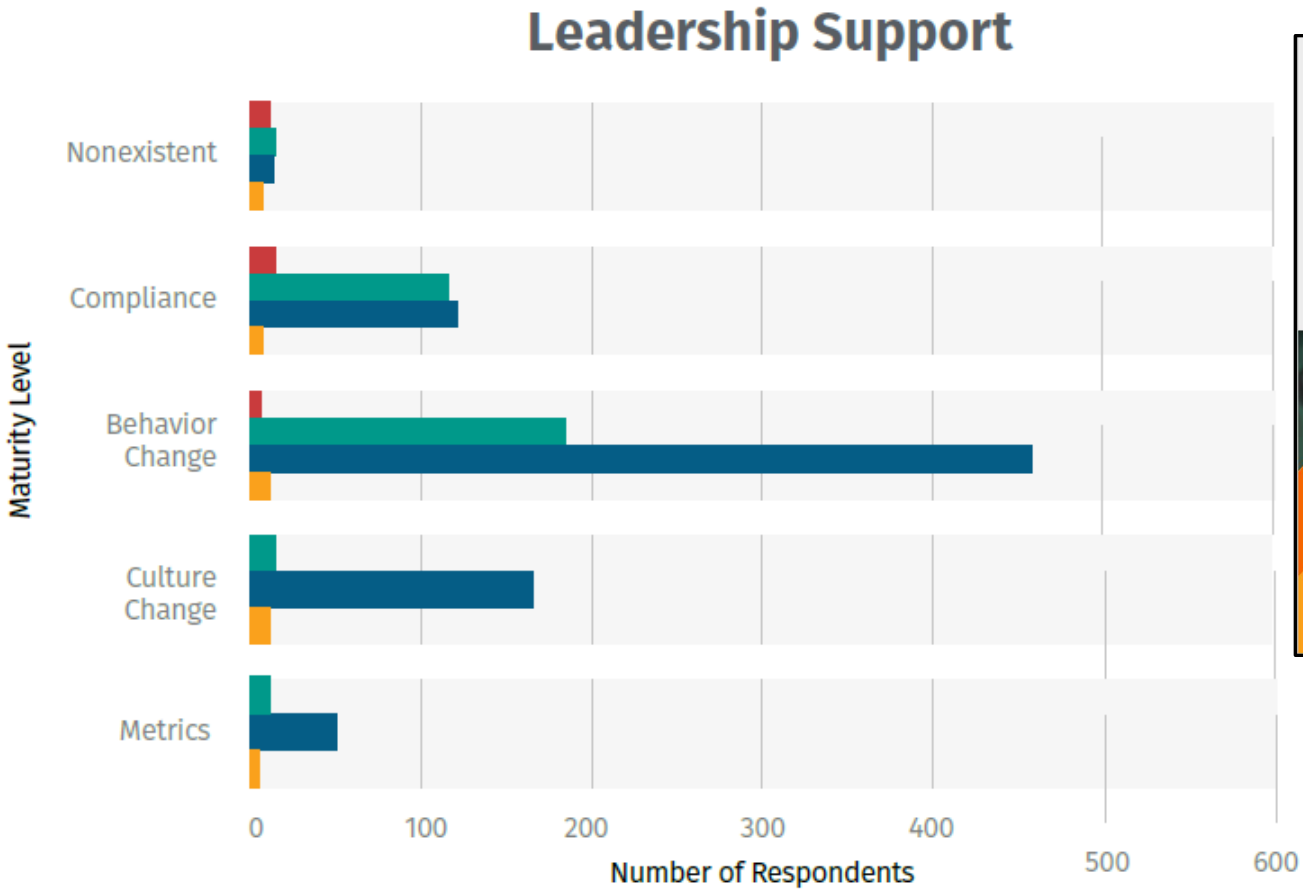
Reported Program Blockers and Supporters

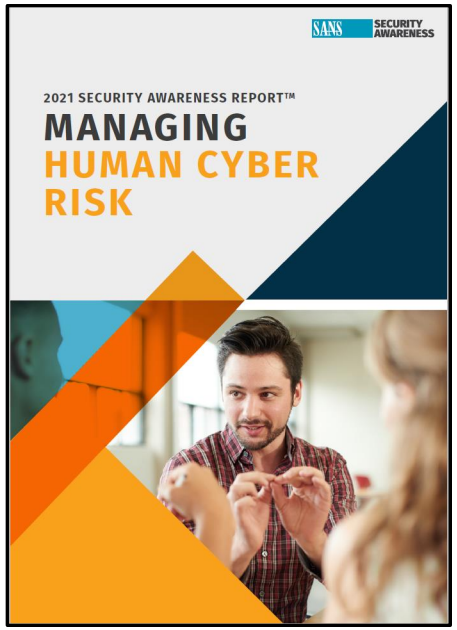


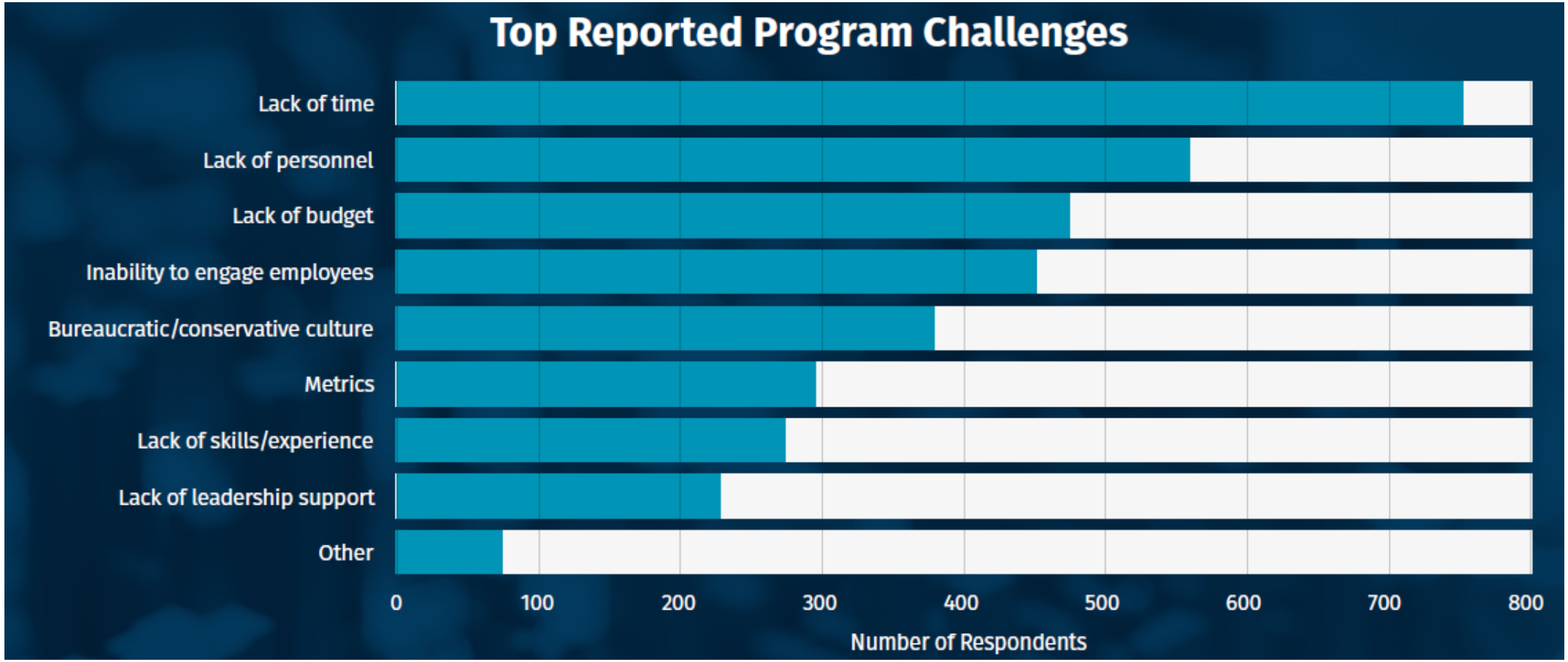


GAINING LEADERSHIP SUPPORT

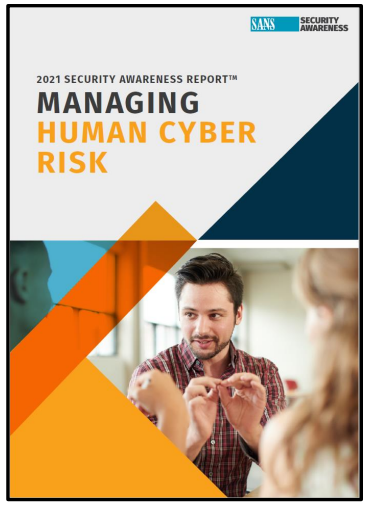
Respondent data shows a correlation between executive support and program maturity. As organizational leaders often decide on critical program resourcing, identification of program goals, training time allocation, and program enforceability, executive support is a key ingredient in program success.



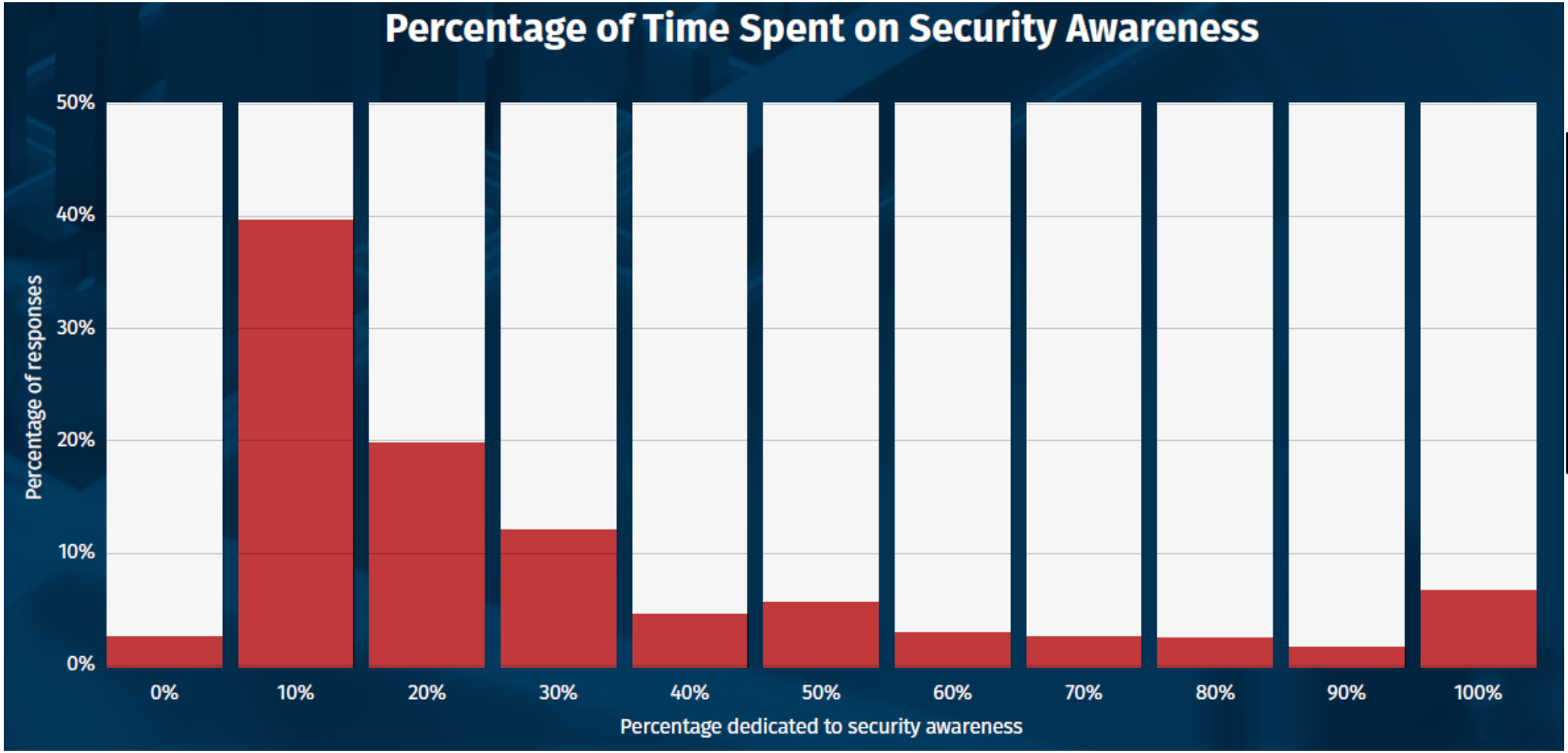


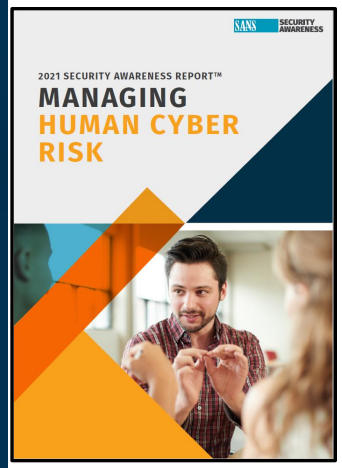


SANS SECURITY AWARENESS



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
Percentage of responses
50%
40%
30%
20%
10%
0%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Percentage dedicated to security awareness

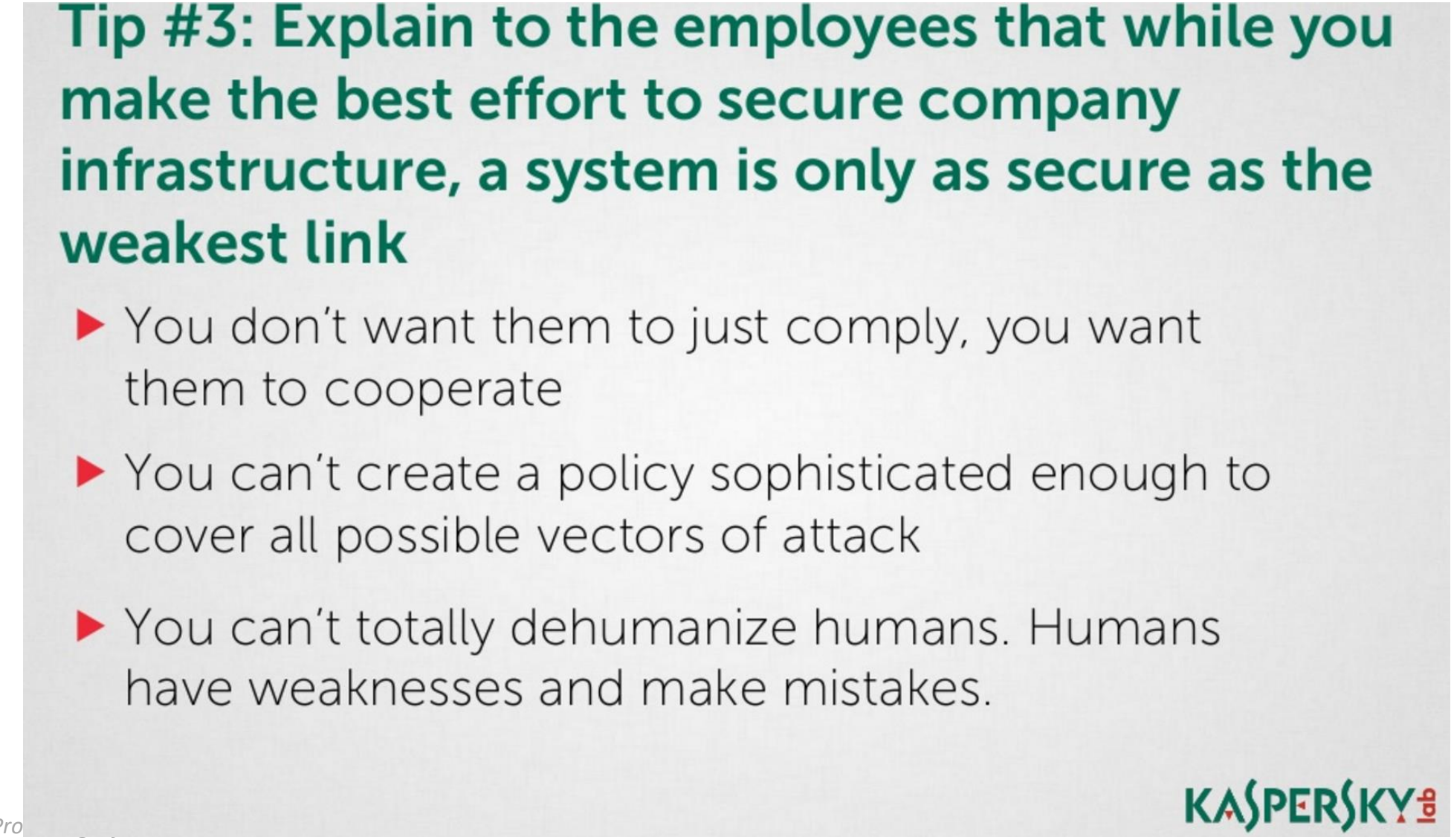

SANS SECURITY AWARENESS
2021 SECURITY AWARENESS REPORT™
MANAGING
HUMAN CYBER
RISK


Security Awareness Team Size, Correlated by Maturity Level
Total
number of full-time employees on security awareness team
4
3.5
3
2.5
2
1.5
1
0.5
0
Non-existent
Compliance-focused
Promoting Awareness & Behavior Change
Long-Term Sustainment & Culture Change
Metrics Framework

What should be in an information security training course ?

- Create a course outline of topics
- Prioritize the topics for teaching the course

Training courses examples…



Training course content example

A. Physical security
B. Desktop security
C. Wireless Networks and Security
D. Password security
E. Phishing
F. Hoaxes
G. Malware
    1. Viruses
    2. Worms
    3. Trojans
    4. Spyware and Adware
H. File sharing and copyright

Brodie, C. (2009), “The Importance of Security Awareness Training”, SANS Institute InfoSec Reading Room, SANS Institute

Training course content example

A. **Password safety and security**
B. Email safety and security
C. Desktop security
D. FERPA Issues (i.e. student information security)
E. Acceptable Use Policy

Fowler, B.T. (2008), “Making Security Awareness Efforts Work for You”, SANS Institute InfoSec Reading Room, SANS Institute

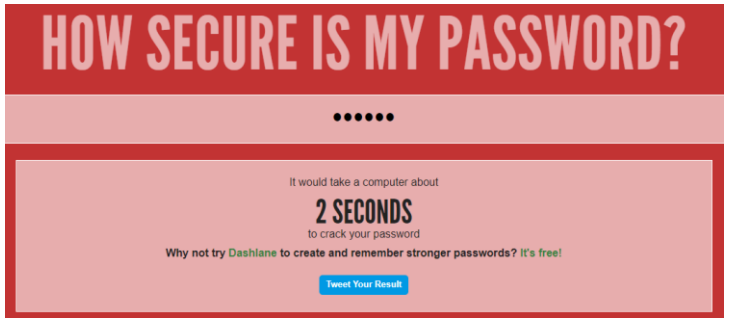
Training course content example…

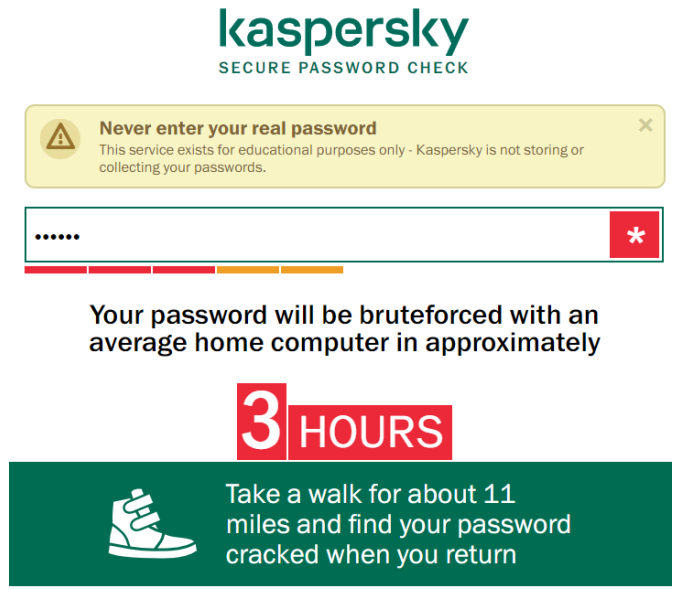
Password safety and security

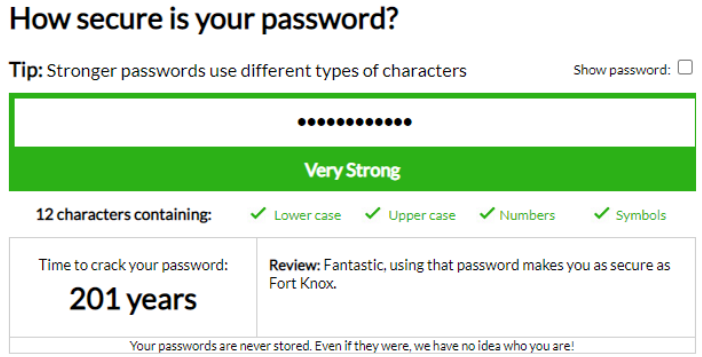
- 80% of hacking related data breaches involve compromised and weak credentials (login and password)
- 29% of all breaches involve the use of stolen credentials

  2019 Verizon Data Breach Investigations Report
- Security policies need to cover both computer and voice mail passwords

- Every employee should be instructed in how to devise a difficult-to-guess password



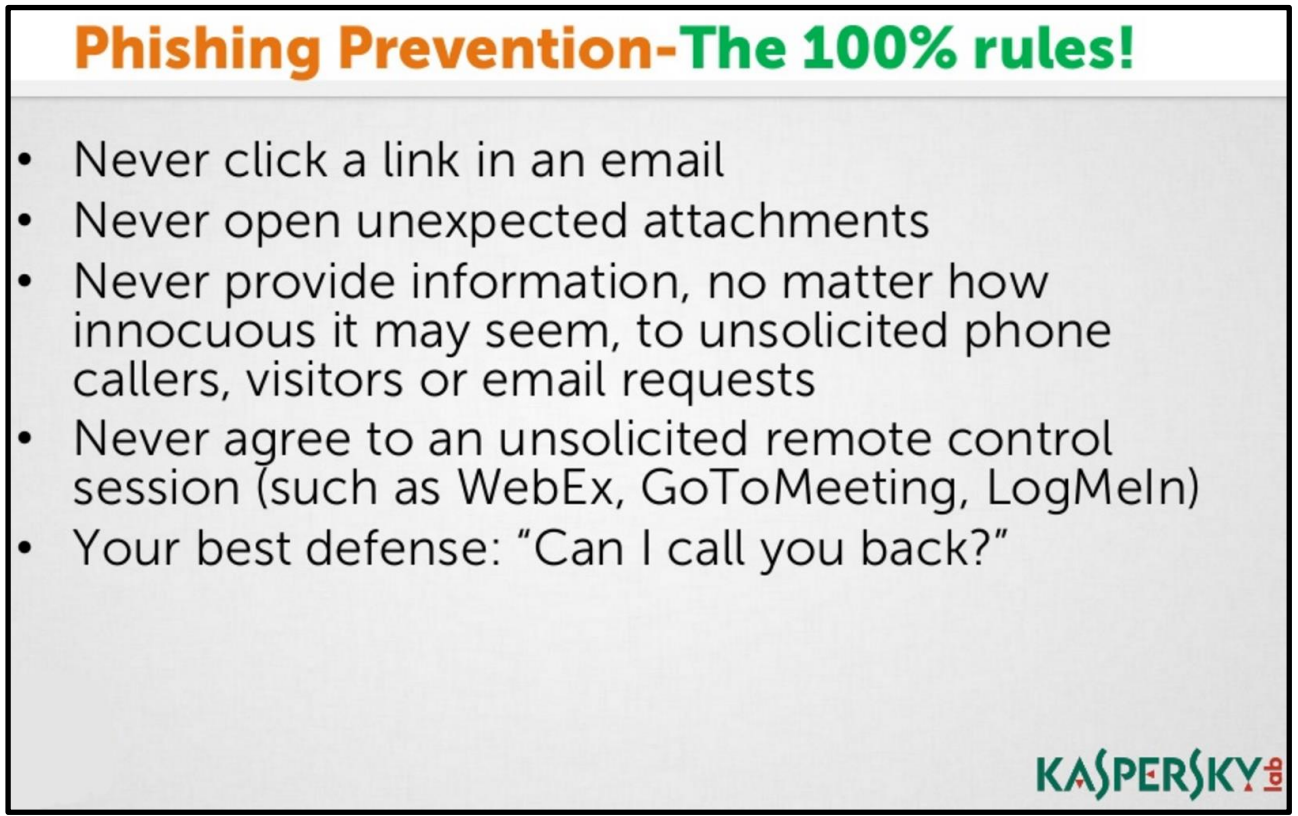




Training course content

Email and Voicemail

- Email usage policy, including the safeguards to prevent malicious code attacks including viruses, worms, and Trojan Horses
- Best security practices of voice mail usage



Training course content

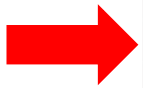
Every employee should know their responsibility to comply with the policies and the consequences for non-compliance

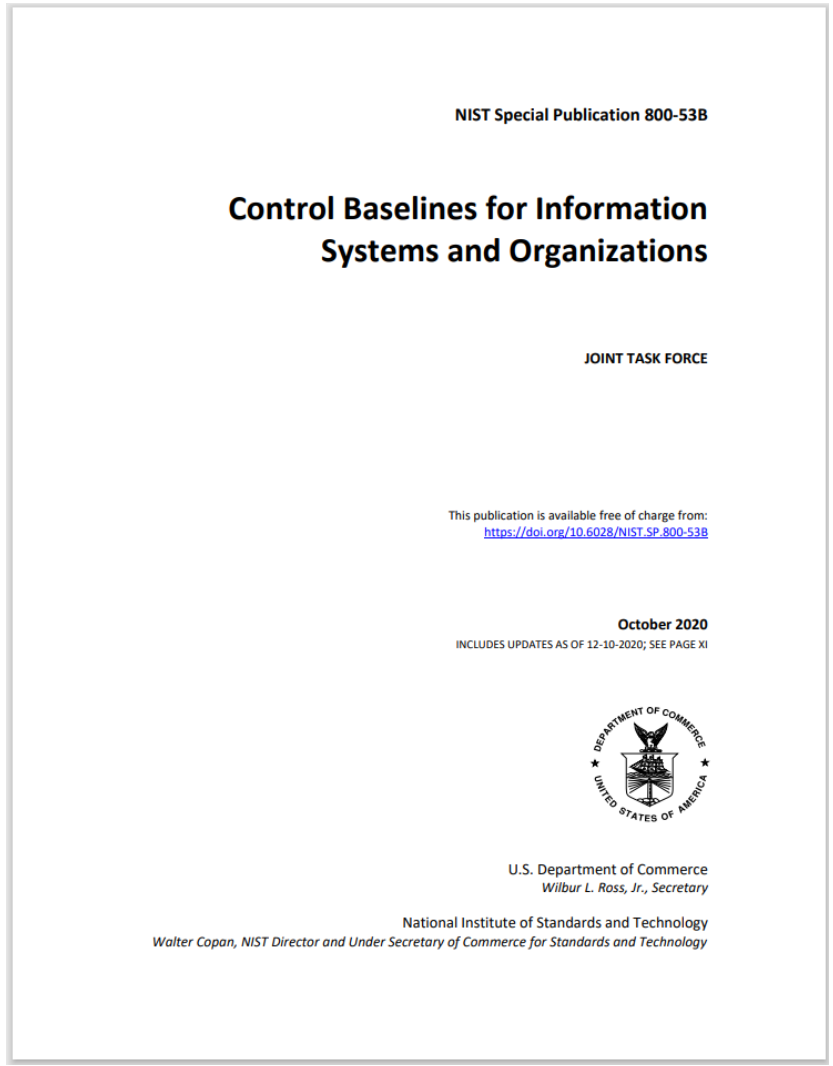
Handling sensitive information

- How to determine the classification of information and the proper safeguards for protecting sensitive information
- The procedure for disclosing sensitive information or materials
- Proper disposal of sensitive documents and computer media that contain, or have at any time in the past contained, confidential materials
- …

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	Policy and Procedures	x	x	x	x
AT-2	Literacy Training and Awareness	x	x	x	x
AT-2(2)	INSIDER THREAT		x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x
AT-3	Role-Based Training	x	x	x	x
AT-4	Training Records	x	x	x	x





NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Social Engineering

- Humans are a key driver of 82% of breaches (Verizon 2022 DBIR, page 8), and social engineering is responsible for a large percentage of these breaches
- Malware and stolen credentials are used as a second step after a social attack gets the threat actor in the door
- This is why having a strong security awareness program is important

These attacks split between Phishing and convincing Pretexting attacks, and are associated with business email compromises

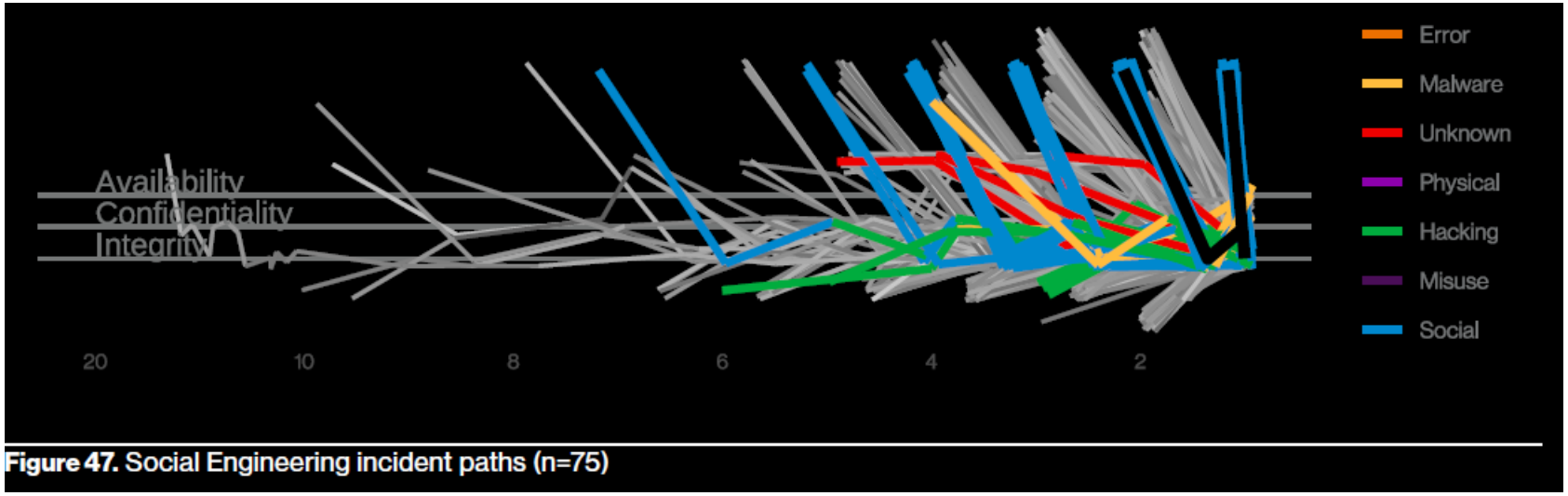
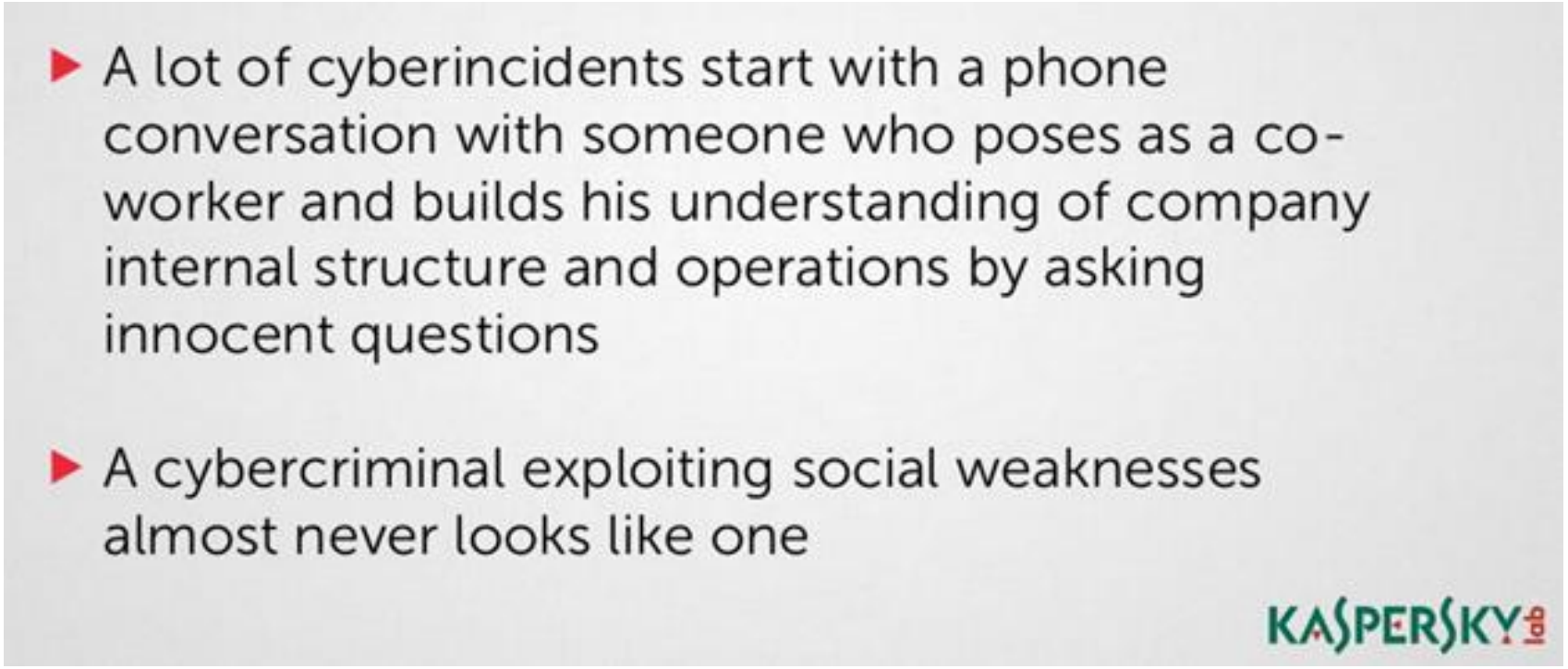


Figure 47. Social Engineering incident paths (n=75)

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…)



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

What is “just in time training?”

“Just in time training…”

Data from network incident reporting tools, such as security and information event management (SIEM) systems and data loss prevention(DLP) software… helps understand prevalence of data handling issues

User behavior analytics (UBA) and user entity behavioral analytics (UEBA) provides a way to parse through information collected by SIEM and DLP

UEBA can help provide “just in time training” as a mistake is made

- *UEBA might identify Jane Doe saving a company document to an unapproved internet site (e.g. Dropbox, Box or Google Drive) and deliver a system-generated pop-up that reminds her of the company’s policy on storing company documents in an authorized ecosystem….*

Pendergast, T. (2016) “How to Audit the Human Element and Assess Your Organization’s Security Risk”, ISACA Journal, Volume 5 pp. 20-24

“Just in time training…”

- *If Jane does it again, the system then might provide a quick video on the reasons why it is best to avoid an unapproved cloud storage system.*

- *Months later, if Jane makes the same mistake again, she might be automatically enrolled in a 15-minute course on approved cloud storage and the appropriate way to store company documents. This is a perfect example of delivering the right training to the right person at the right time.”*

Pendergast, T. (2016) “How to Audit the Human Element and Assess Your Organization’s Security Risk”, ISACA Journal, Volume 5 pp. 20-24

Agenda

- ✓ Awareness and Training Controls
- ✓ Creating a Security Aware Organization
  - ✓ Awareness and Training InfoSec Controls
  - ✓ The Threat landscape
  - ✓ Employee risk
  - ✓ Training course content (examples)
- Test Taking Tip
- Quiz

Test Taking Tip

- If you don't know the answer … guess and then move on -

Your score will be higher if you guess and move on even if your guess is wrong

Here's why:

- Most certification tests do not penalize for wrong answers. That is, they only count the number of correct answers in computing the score
- In a 4 option multiple choice test, guessing at questions to which you do not know the answer is likely to get you an additional right answer ¼ of the time
- Guessing, and then moving on, gives you time to answer the questions that you do know, raising your score

Quiz and Solutions

1. An information system (IS) auditor is reviewing a third-party agreement for a new cloud-based accounting service provider. Which of the following considerations is the MOST important with regard to the privacy of the accounting data?
    a. Data retention, backup and recovery
    b. Return or destruction of information
    c. Network and intrusion detection
    d. A patch management process

1. An information system (IS) auditor is reviewing a third-party agreement for a new cloud-based accounting service provider. Which of the following considerations is the MOST important with regard to the privacy of the accounting data?
    a. Data retention, backup and recovery
    b. Return or destruction of information
    c. Network and intrusion detection
    d. A patch management process

2. During an IS risk assessment of a health care organization regarding protected health care information (PHI), an IS auditor interviews IS management. Which of the following findings from the interviews would be of MOST concern to the IS auditor?
    a. The organization does not encrypt all of its outgoing email messages
    b. Staff have to type "[PHI]" in the subject field of email messages to be encrypted
    c. An individual's computer screen saver function is disabled
    d. Server configuration requires the user to change the password annually

2. During an IS risk assessment of a health care organization regarding protected health care information (PHI), an IS auditor interviews IS management. Which of the following findings from the interviews would be of MOST concern to the IS auditor?
    a. The organization does not encrypt all of its outgoing email messages
    b. Staff have to type "[PHI]" in the subject field of email messages to be encrypted
    c. An individual's computer screen saver function is disabled
    d. Server configuration requires the user to change the password annually

3. Which of the following is the responsibility of information asset owners?
    a. Implementation of information security within applications
    b. Assignment of criticality levels to data
    c. Implementation of access rules to data and programs
    d. Provision of physical and logical security for data

3. Which of the following is the responsibility of information asset owners?
    a. Implementation of information security within applications
    b. Assignment of criticality levels to data
    c. Implementation of access rules to data and programs
    d. Provision of physical and logical security for data

4. With the help of a security officer, granting access to data is the responsibility of:
    a. Data owners
    b. Programmers
    c. Systems analysts
    d. Librarians

4. With the help of a security officer, granting access to data is the responsibility of:
    a. Data owners
    b. Programmers
    c. Systems analysts
    d. Librarians

5. The FIRST step in data classification is to
    a. Establish ownership
    b. Perform a criticality analysis
    c. Define access rules
    d. Create a data dictionary

5. The FIRST step in data classification is to
    a. Establish ownership
    b. Perform a criticality analysis
    c. Define access rules
    d. Create a data dictionary

6. Which of the following would MOST effectively reduce social engineering incidents?
    a. Security awareness training
    b. Increased physical security measures
    c. Email monitoring policy
    d. Intrusion detection systems

6. Which of the following would MOST effectively reduce social engineering incidents?
    a. Security awareness training
    b. Increased physical security measures
    c. Email monitoring policy
    d. Intrusion detection systems

7. Which of the following acts as a decoy to detect active Internet attacks?
    a. Honeypots
    b. Firewalls
    c. Trapdoors
    d. Traffic analysis

7. Which of the following acts as a decoy to detect active Internet attacks?
    a. Honeypots
    b. Firewalls
    c. Trapdoors
    d. Traffic analysis

8. Which of the following is the BEST way for an IS auditor to determine the effectiveness of a security awareness and training program?
    a. Review the security training program
    b. Ask the security administrator
    c. Interview a sample of employees
    d. Review the security reminders to employees

8. Which of the following is the BEST way for an IS auditor to determine the effectiveness of a security awareness and training program?
    a. Review the security training program
    b. Ask the security administrator
    c. Interview a sample of employees
    d. Review the security reminders to employees

9. As his company's Chief Information Security Officer (CISO), George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?
    a. threats x vulnerability X asset value = residual risk
    b. SLE x frequency = ALE, which is equal to residual risk
    c. (threats x vulnerability x asset value) x control gap = residual risk
    d. (total risk – asset value) x countermeasures = residual risk

9. As his company's Chief Information Security Officer (CISO), George needs to demonstrate to the Board of Directors the necessity of a strong risk management program. Which of the following should George use to calculate the company's residual risk?
    a. threats x vulnerability X asset value = residual risk
    b. SLE x frequency = ALE, which is equal to residual risk
    c. (threats x vulnerability x asset value) x control gap = residual risk
    d. (total risk – asset value) x countermeasures = residual risk

10. Which of the following is not included in a risk assessment?
    a. Discontinuing activities that introduce risk
    b. Identifying assets
    c. Identifying threats
    d. Analyzing risk in order of cost or criticality

10. Which of the following is not included in a risk assessment?
    a. Discontinuing activities that introduce risk
    b. Identifying assets
    c. Identifying threats
    d. Analyzing risk in order of cost or criticality

Agenda

- ✓ Awareness and Training Controls
- ✓ Creating a Security Aware Organization
  - ✓ Awareness and Training InfoSec Controls
  - ✓ The Threat landscape
  - ✓ Employee risk
  - ✓ Training course content (examples)
- ✓ Test Taking Tip
- ✓ Quiz

Protecting Information Assets

- Unit# 5 -

Creating a Security Aware Organization