

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
- Test Taking Tip
- Quiz

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

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](#)

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

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



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 security categorization of the Financial Information Management System...

Informaton Type	IMPACT RATINGS			
	Confidentiality	Integrity	Availability	Security Categorization
Assets and Liability Management	Low	Low	Low	Low
Reporting and Information	Low	Moderate	Low	Moderate
Funds Control	Moderate	Moderate	Low	Moderate
Accounting	Low	Moderate	Low	Moderate
Payments	Low	Moderate	Low	Moderate
Collecitons and Receivables	Low	Moderate	Low	Moderate
Cost Accounting/Performance Measurement	Low	Moderate	Low	Moderate
Overall Categorization:	Moderate	Moderate	Low	Moderate

How would you audit these risk controls?

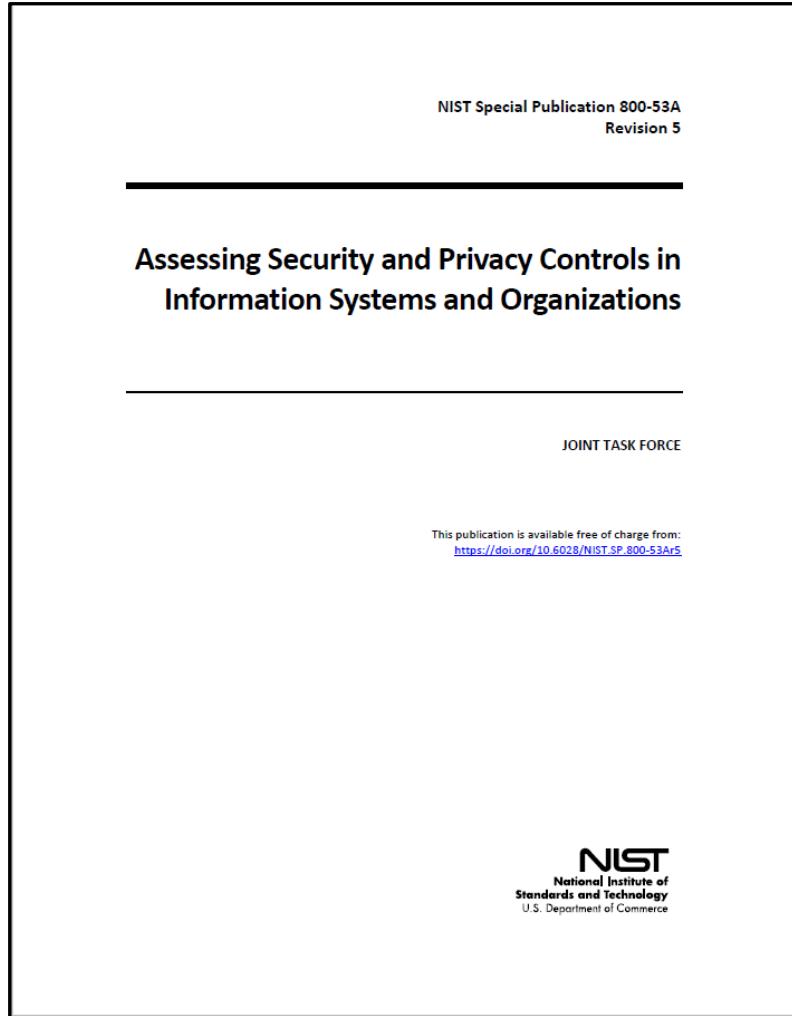


TABLE 3-2: AWARENESS AND TRAINING FAMILY

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				

Class exercise:

Find an audit control checklist for AT-1...

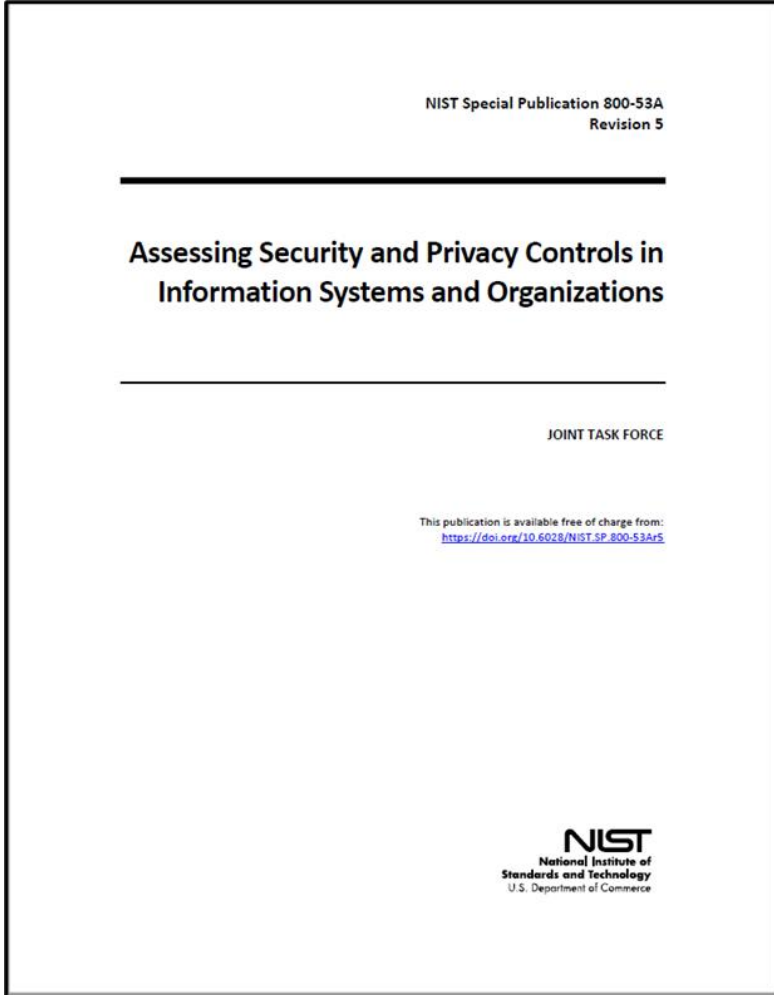


TABLE 3-2: AWARENESS AND TRAINING FAMILY

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: <i>Determine if:</i>	
AT-01_ODP[01]	<i>personnel or roles to whom the awareness and training policy is to be disseminated is/are defined;</i>
AT-01_ODP[02]	<i>personnel or roles to whom the awareness and training procedures are to be disseminated is/are defined;</i>
AT-01_ODP[03]	<i>one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};</i>
AT-01_ODP[04]	<i>an official to manage the awareness and training policy and procedures is defined;</i>
AT-01_ODP[05]	<i>the frequency at which the current awareness and training policy is reviewed and updated is defined;</i>
AT-01_ODP[06]	<i>events that would require the current awareness and training policy to be reviewed and updated are defined;</i>
AT-01_ODP[07]	<i>the frequency at which the current awareness and training procedures are reviewed and updated is defined;</i>
AT-01_ODP[08]	<i>events that would require procedures to be reviewed and updated are defined;</i>
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>


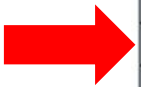
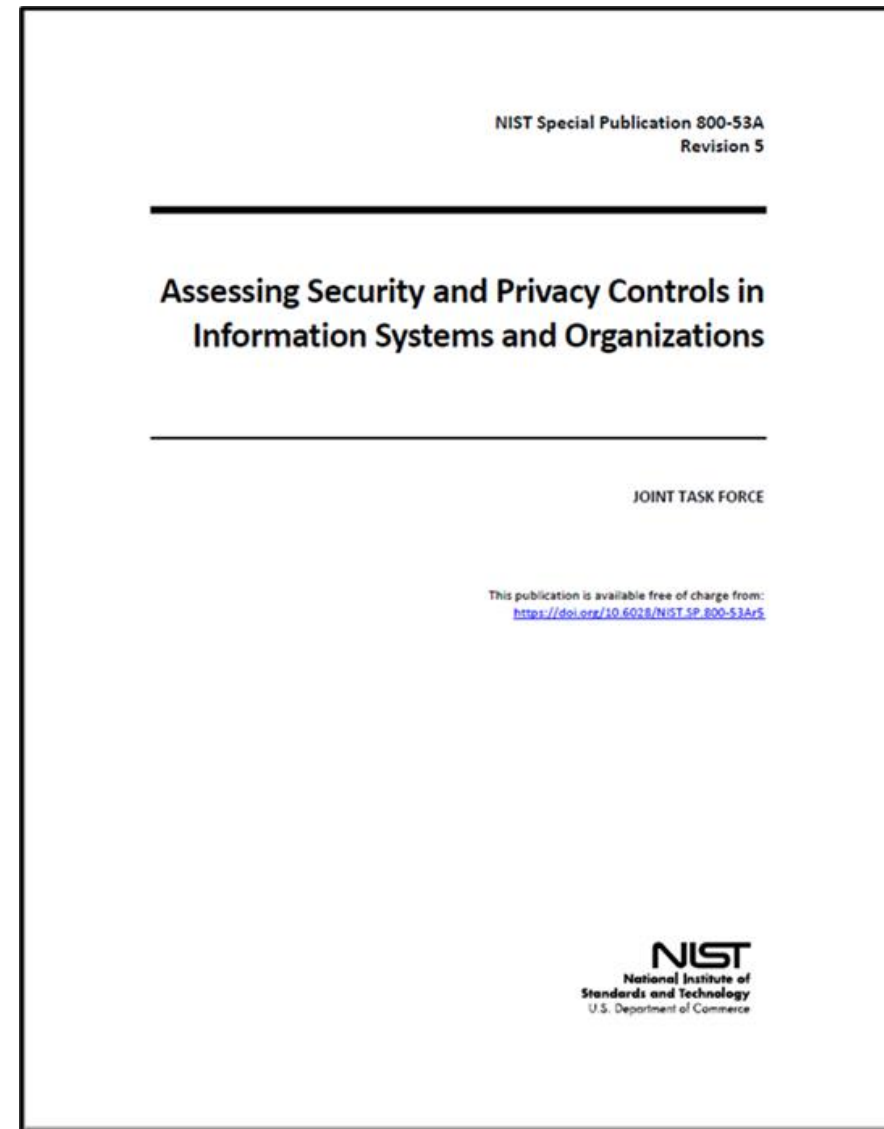


TABLE 3-2: AWARENESS AND TRAINING FAMILY

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 this training at the organization you are auditing?

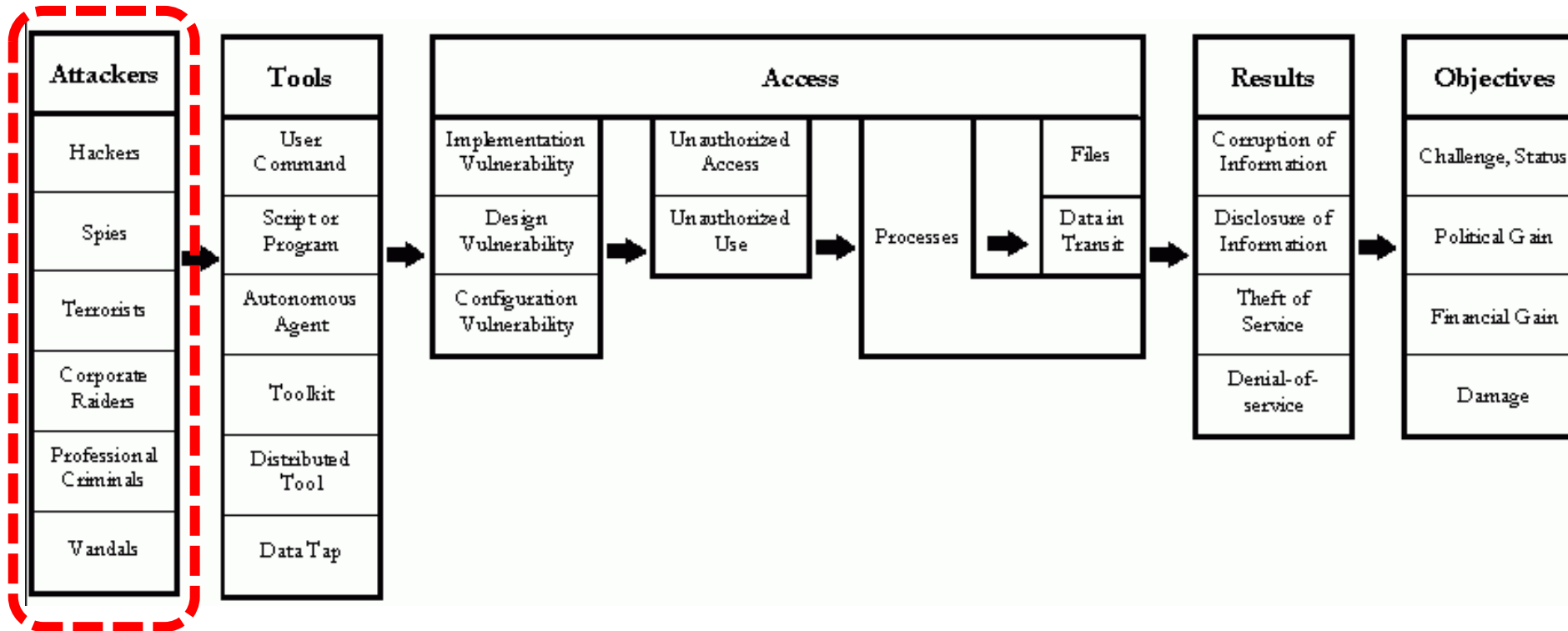


AT-02 LITERACY TRAINING AND AWARENESS	
ASSESSMENT OBJECTIVE: <i>Determine if:</i>	
AT-02_ODP[01]	<i>the frequency at which to provide security literacy training to system users (including managers, senior executives, and contractors) after initial training is defined;</i>
AT-02_ODP[02]	<i>the frequency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

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

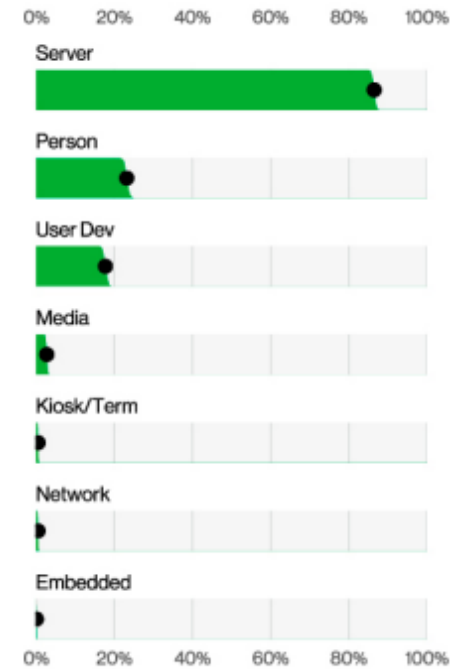
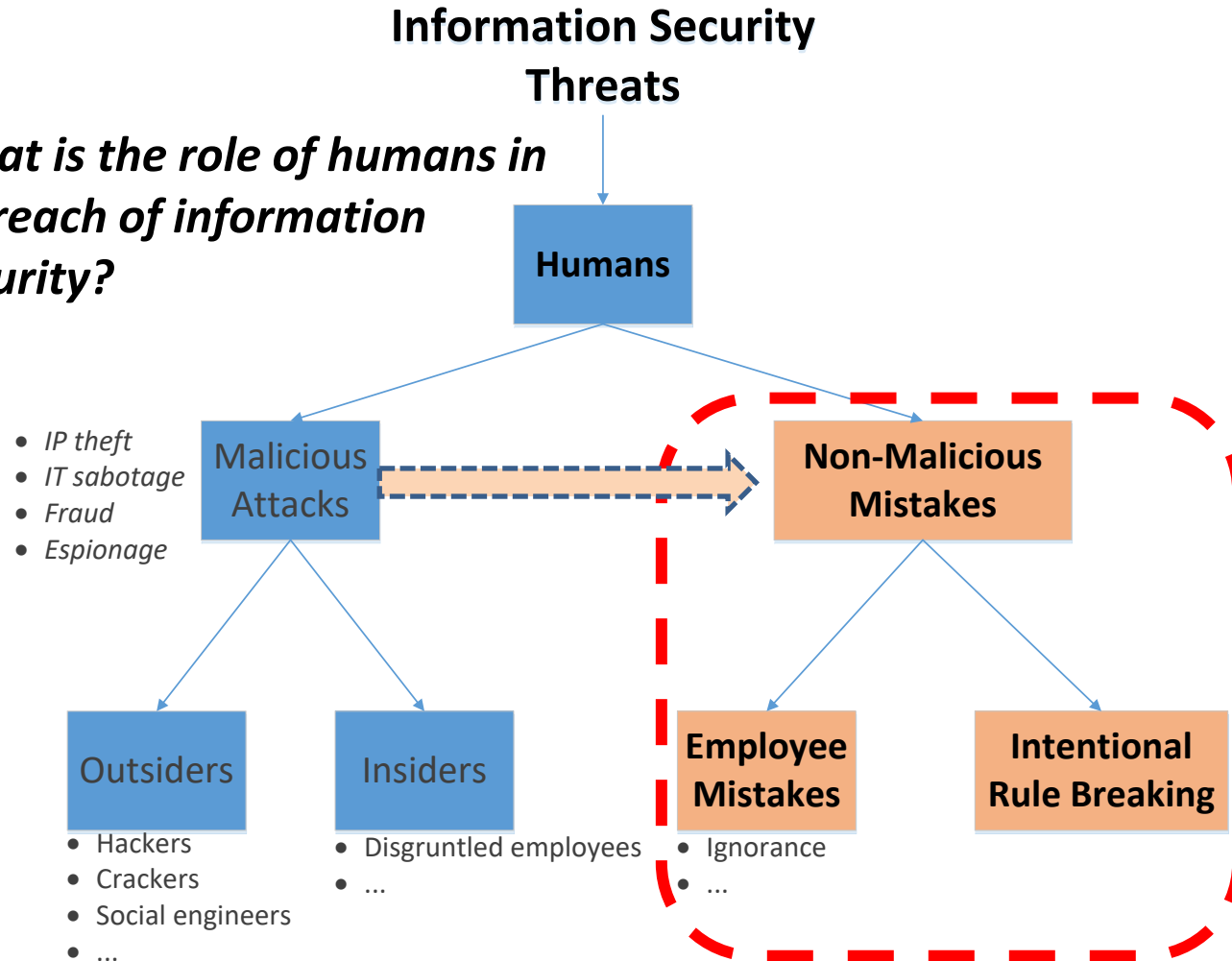


Figure 19. Assets in breaches (n=4,433)

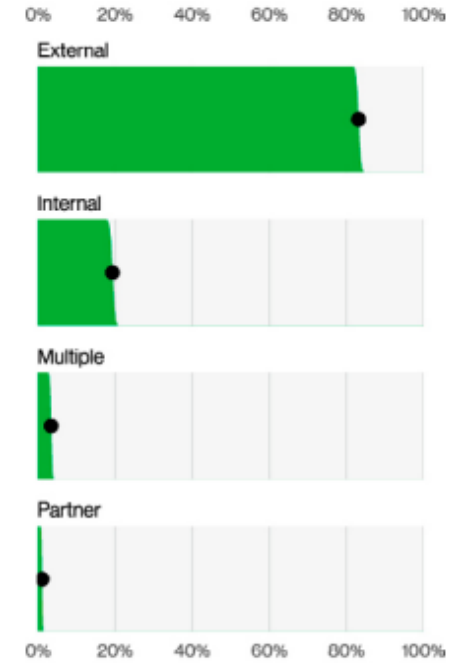
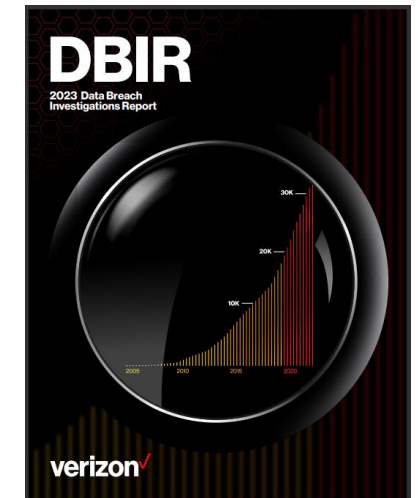


Figure 11. Threat actors in breaches (n=5,177)



What roles do employees play in these attack chains

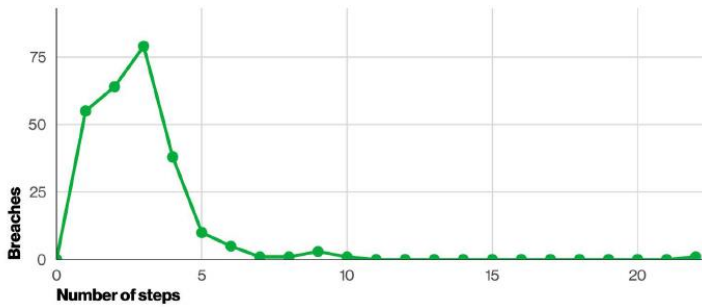
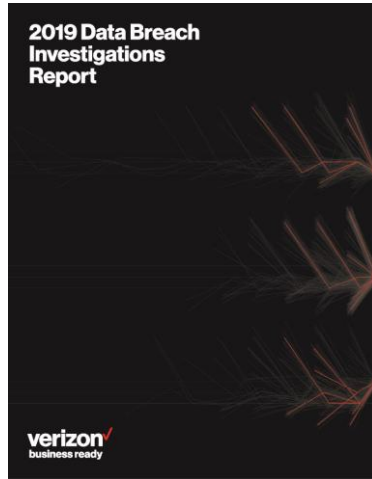


Figure 30. Number of steps per breach in non-Error breaches (n=258)

MIS 5206 Protecting Information Assets

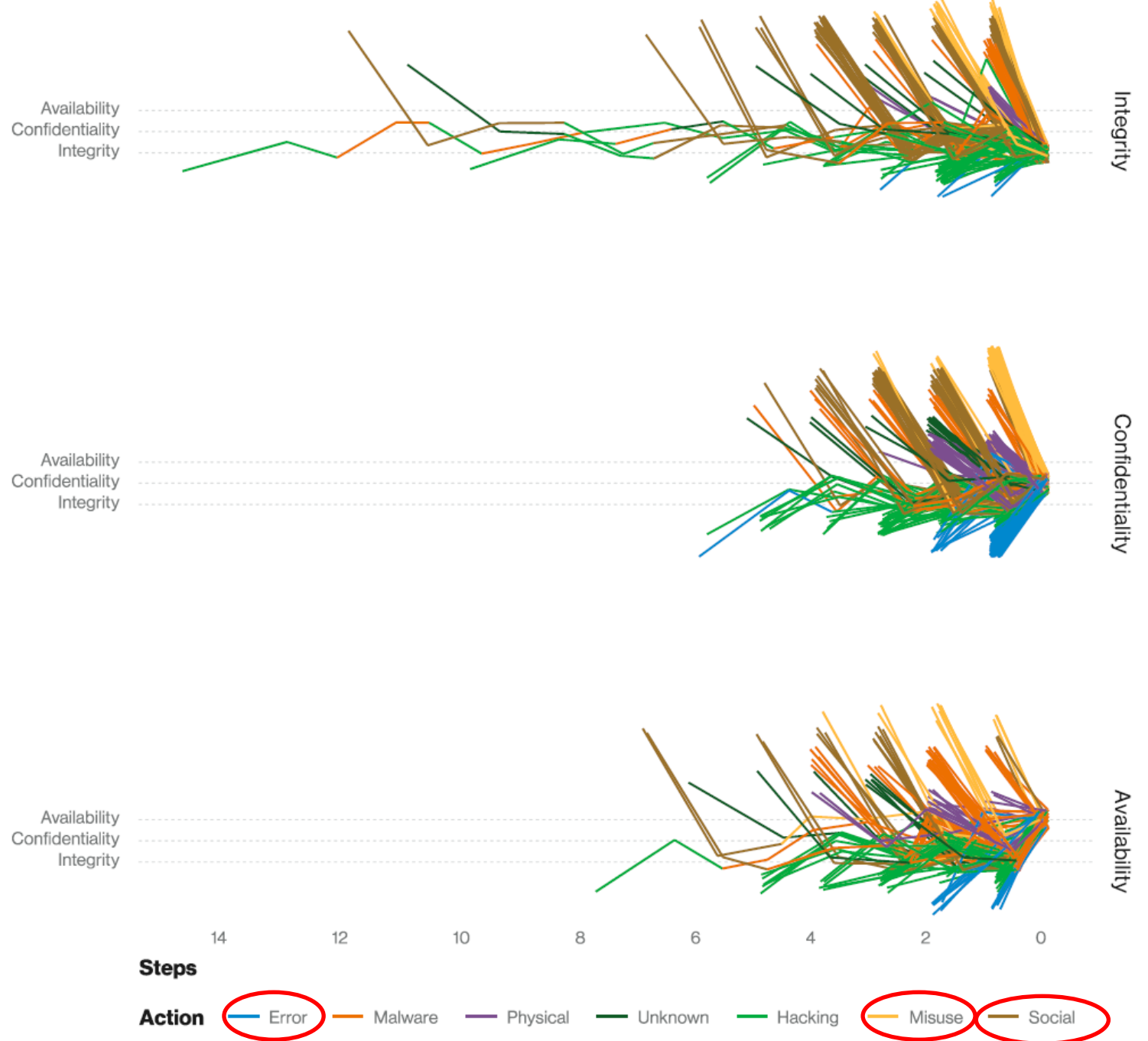
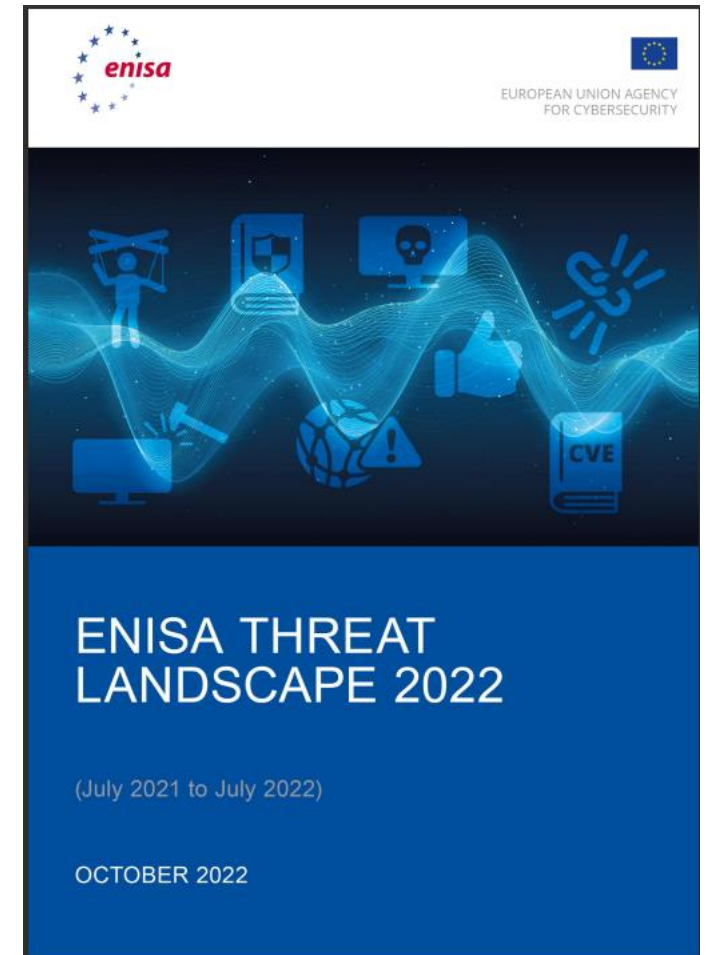
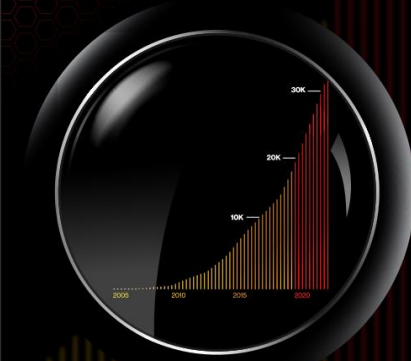


Figure 30. Attack chain by final attribute compromised¹² (n=941)

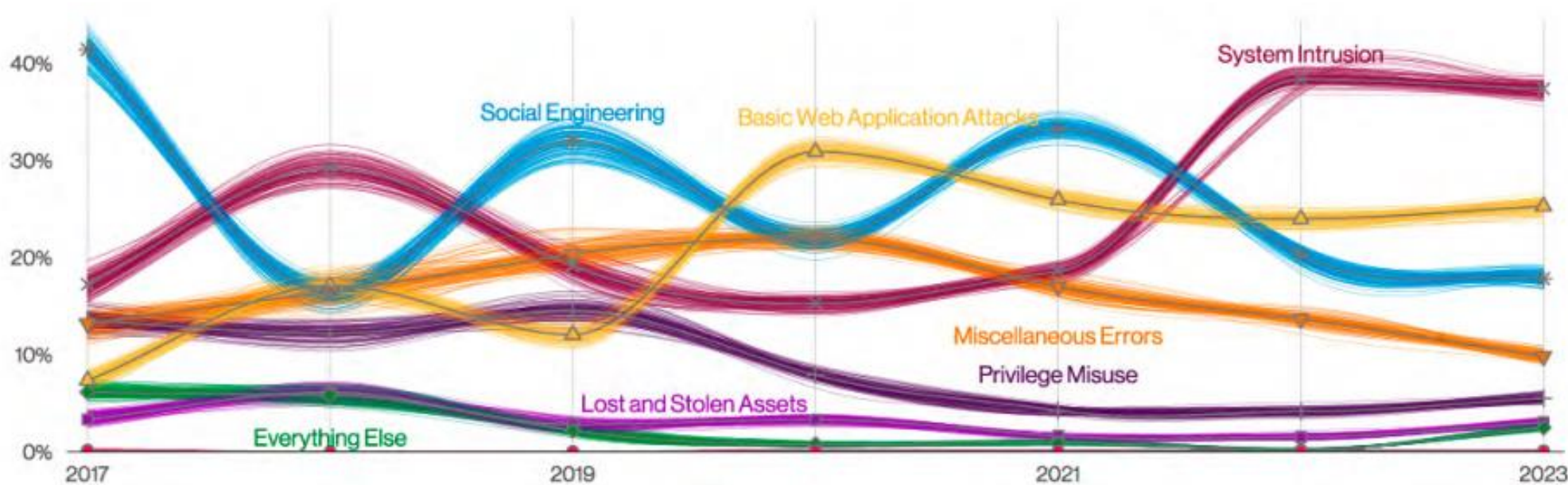
Figure 1: ENISA Threat Landscape 2022 - Prime threats



In which of these threats are humans the vulnerability?



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

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

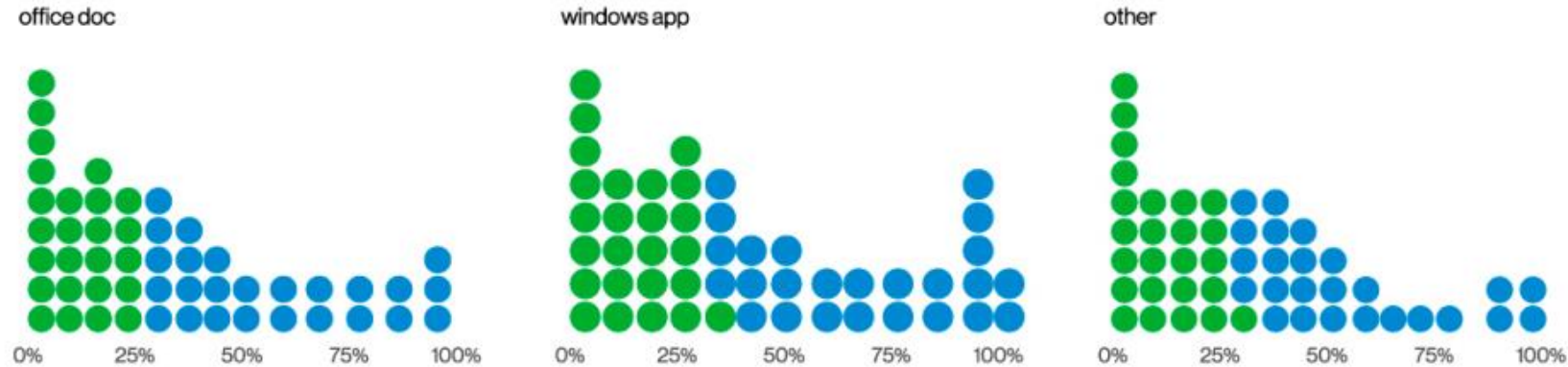
- Organizations must also ensure their security posture is good by:
 - Setting policies, educating staff, and enforcing good security hygiene
 - Taking advantage of the security options that are available
 - Training and testing employees
 - Implementing automated checks to ensure their security posture

Employee Risk

Malware delivery methods

“Malware is largely distributed via email and often comes in the form of Microsoft Office documents. This makes sense when you consider that most of these documents now have the ability to run code on the client system, which is extremely useful if you’re an attacker.”

Malware file types (n=1,756)



Malware delivery methods (n=1,069)

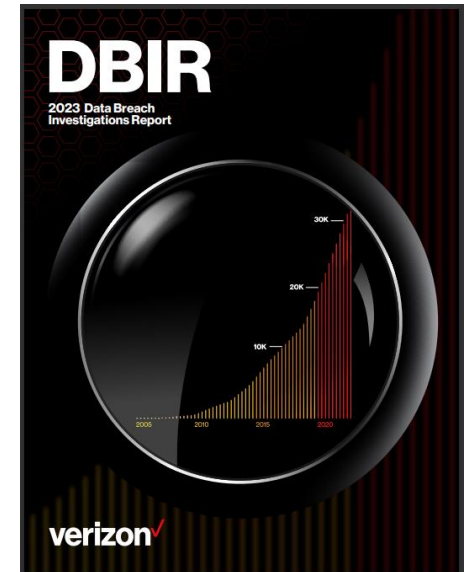
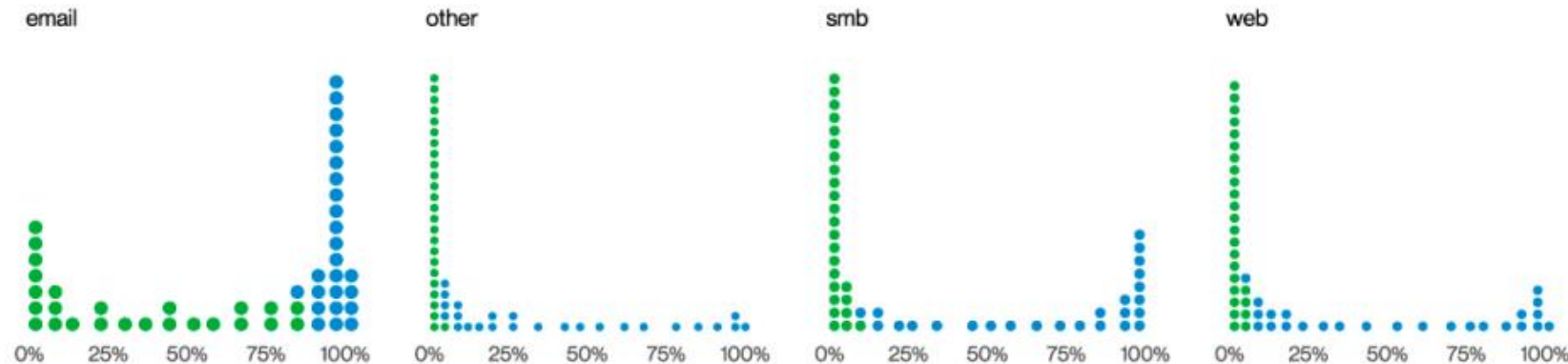
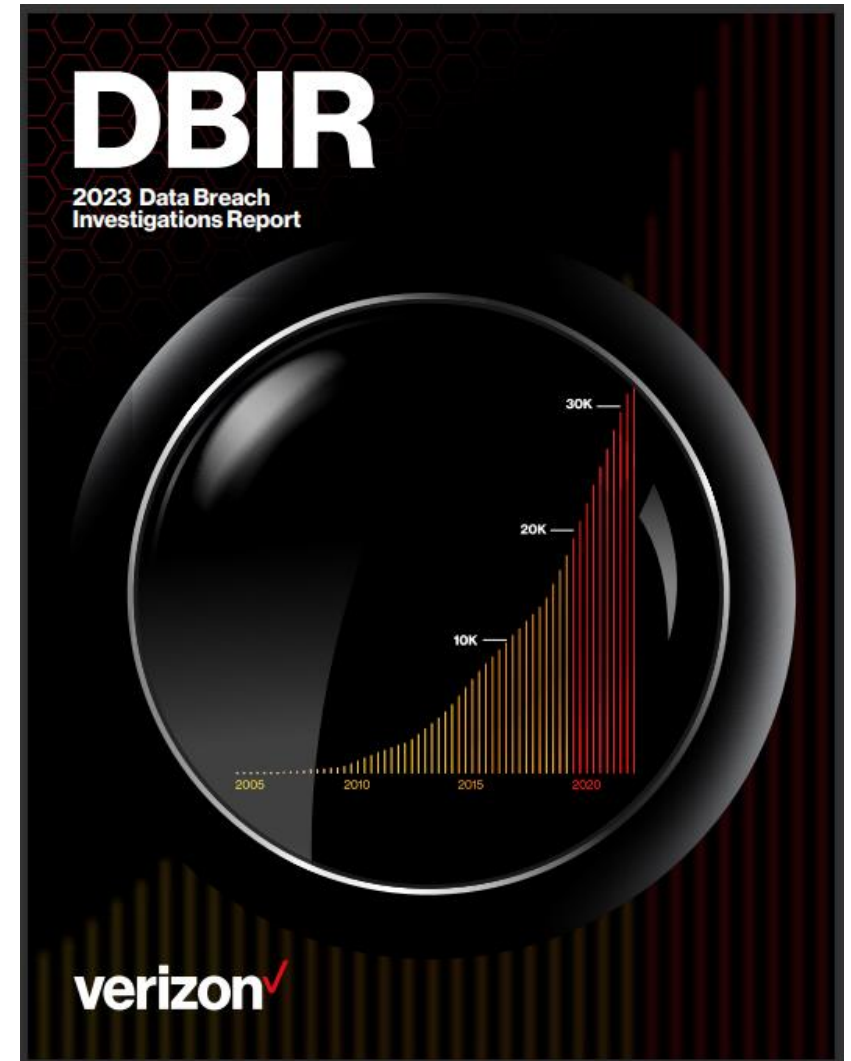


Figure 30. Malware delivery method proportion per organization



Figure 14. Top Action varieties in breaches (n=4,354)



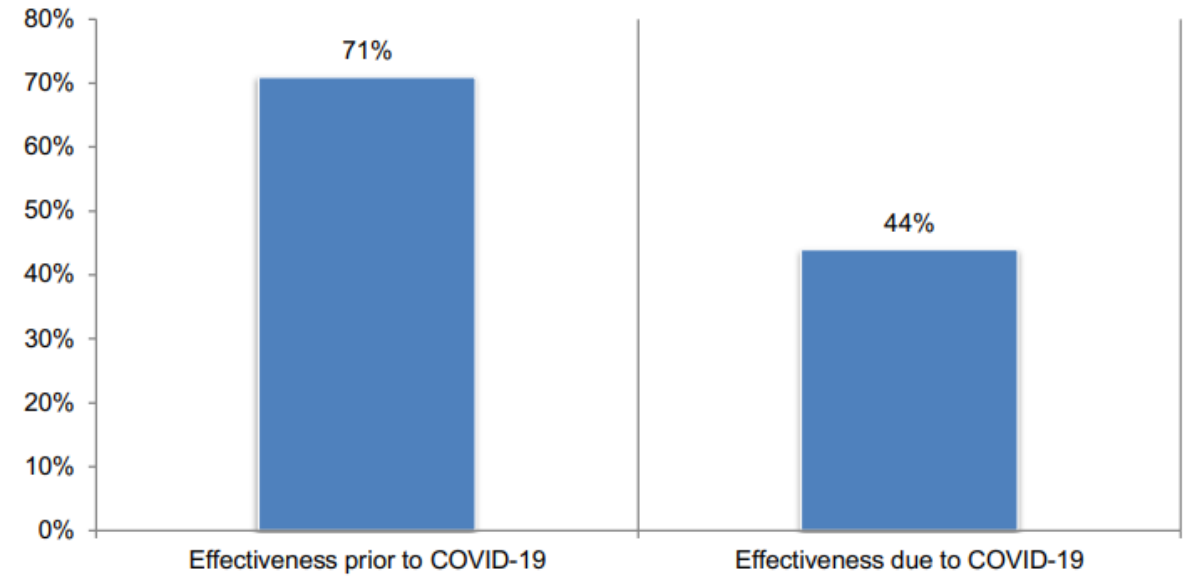
Cybersecurity in the Remote Work Era:

A Global Risk Report

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

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



Cybersecurity in the Remote Work Era:

A Global Risk Report

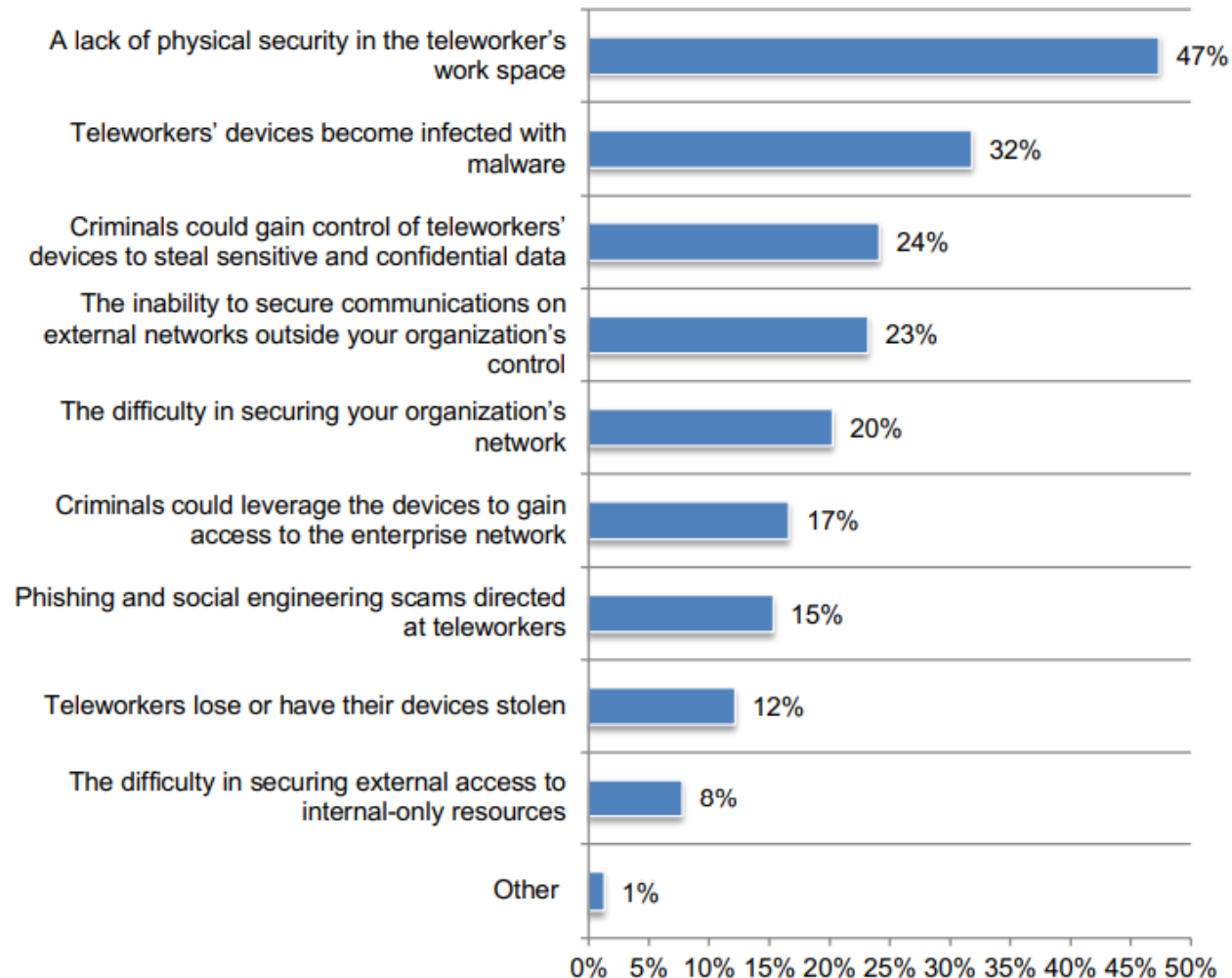
Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC



Ponemon Institute © 2020 Research Report

Figure 3. Security risks organizations are most concerned about

More than one response permitted



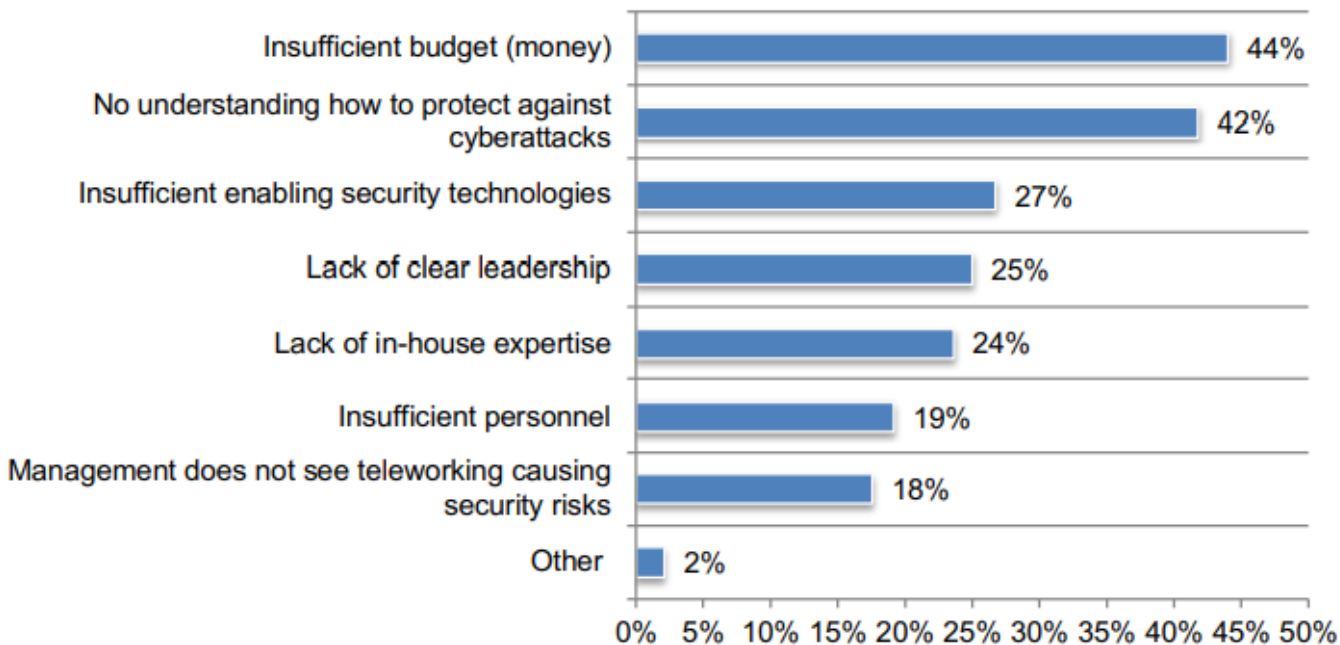
Cybersecurity in the Remote Work Era:

A Global Risk Report

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

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 University's Software Engineering Institute's (SEI) Computer Emergency Response Team (CERT) 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...

“Terrific 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.

- 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 <i>INSIDER THREAT</i>
	<p>ASSESSMENT OBJECTIVE:</p> <p><i>Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.</i></p>
	<p>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</p> <p>Examine: [<i>SELECT FROM:</i> 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].</p> <p>Interview: [<i>SELECT FROM:</i> Organizational personnel that participate in security awareness training; organizational personnel with responsibilities for basic security awareness training; organizational personnel with information security responsibilities].</p>

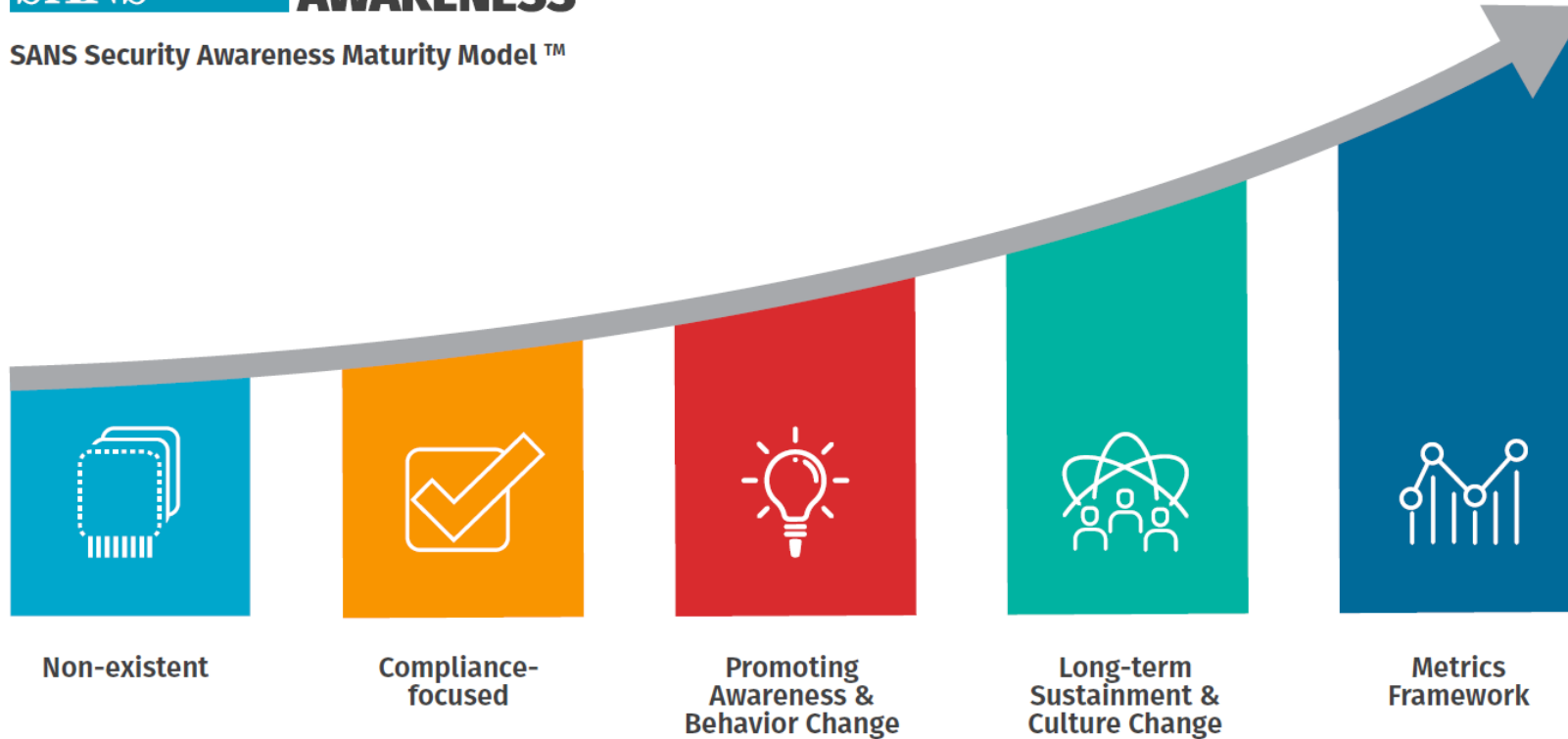
TABLE 3-2: AWARENESS AND TRAINING FAMILY

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?

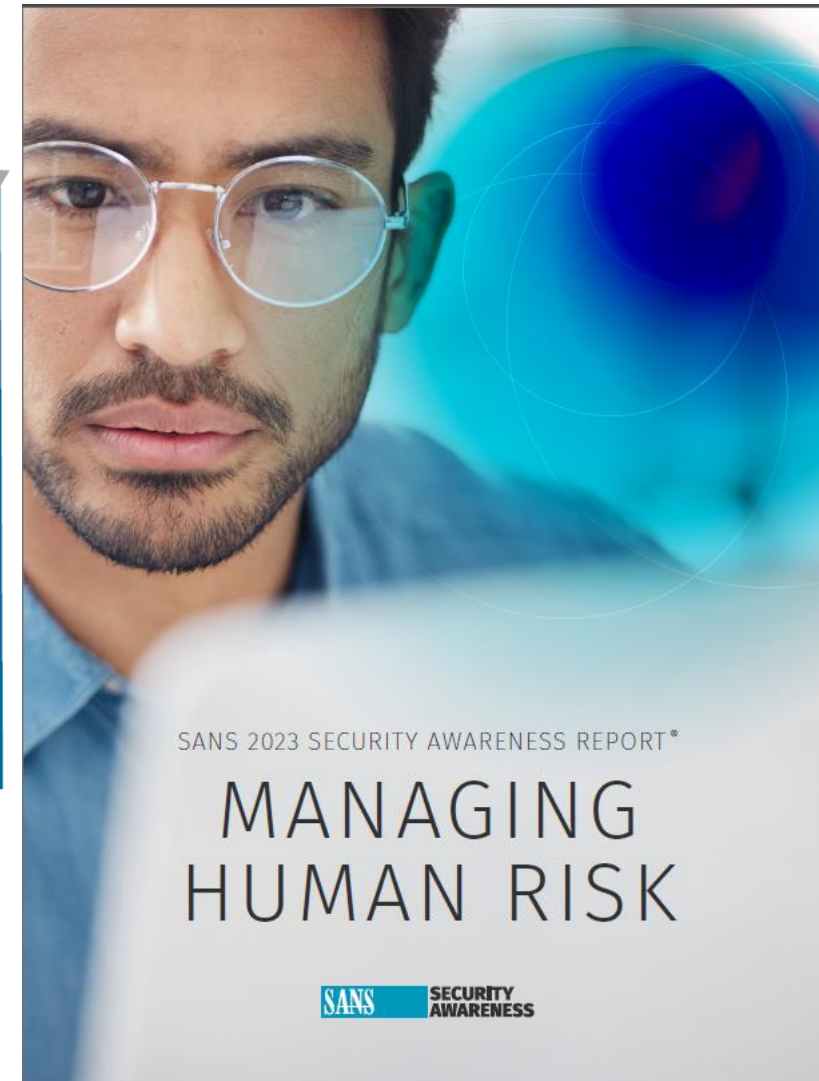


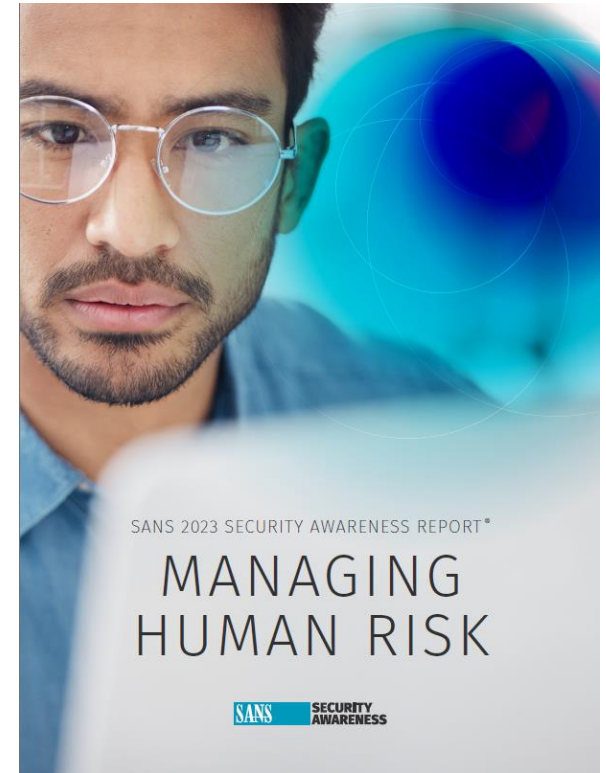
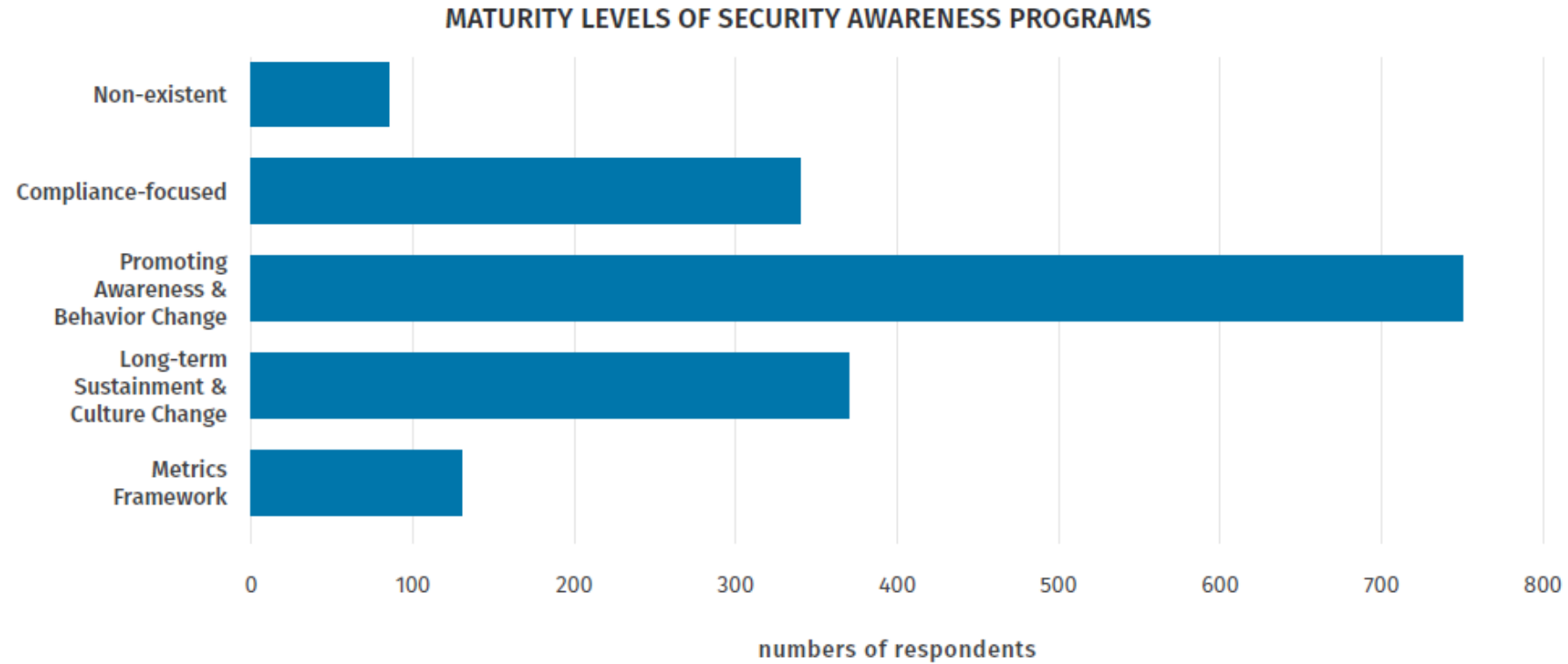
SANS Security Awareness Maturity Model™



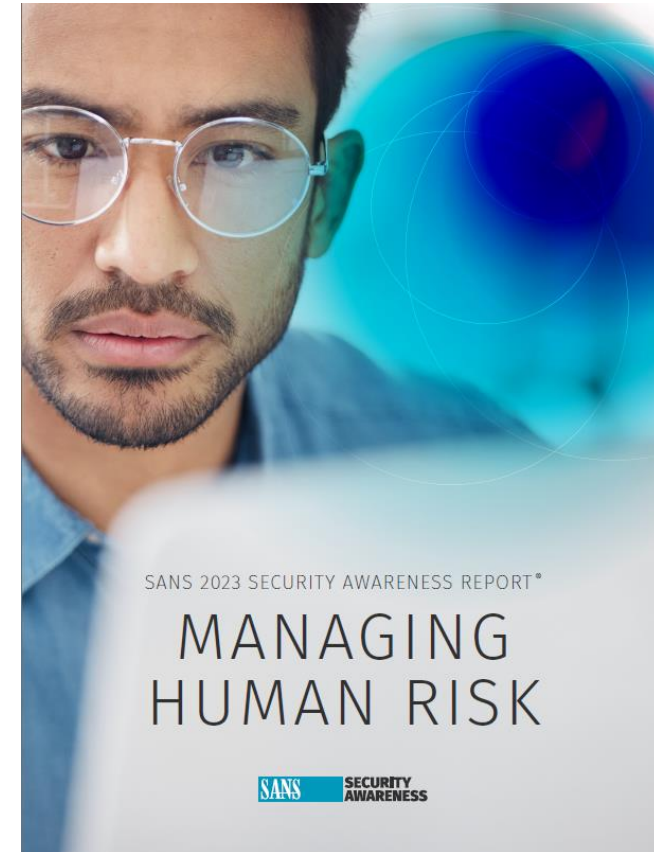
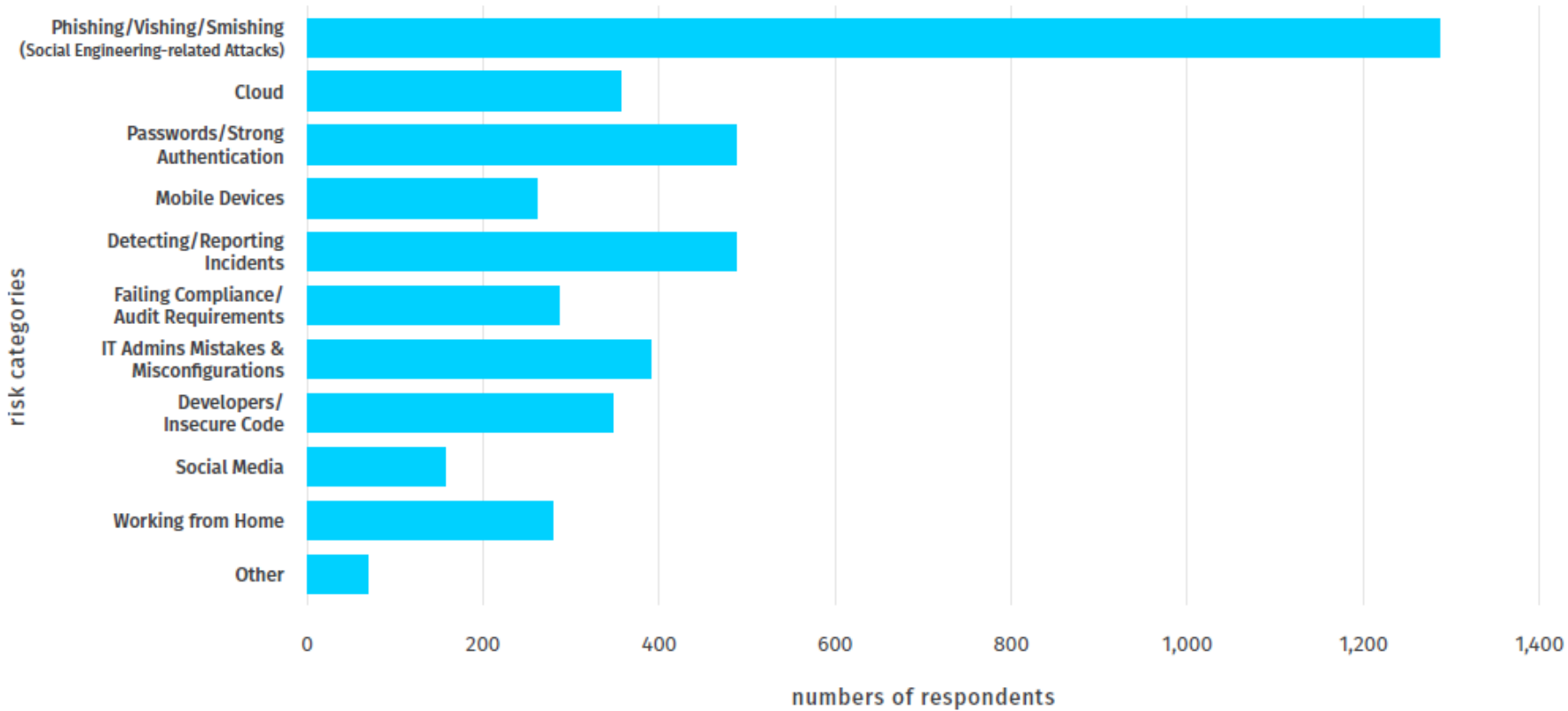
<https://www.sans.org/blog/sans-2022-security-awareness-report/>

MIS 5206 Protecting Information Assets

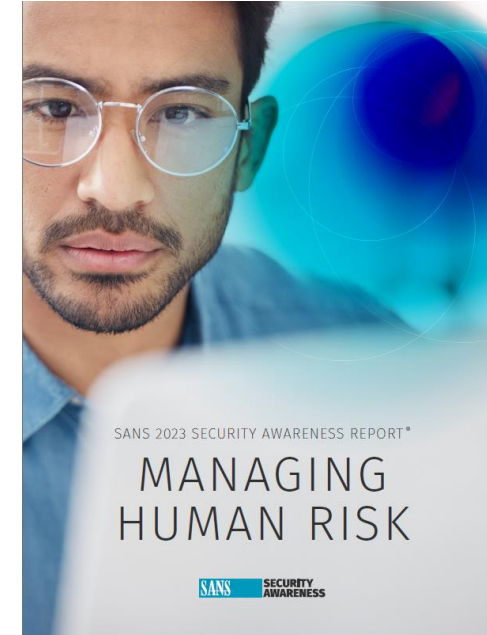
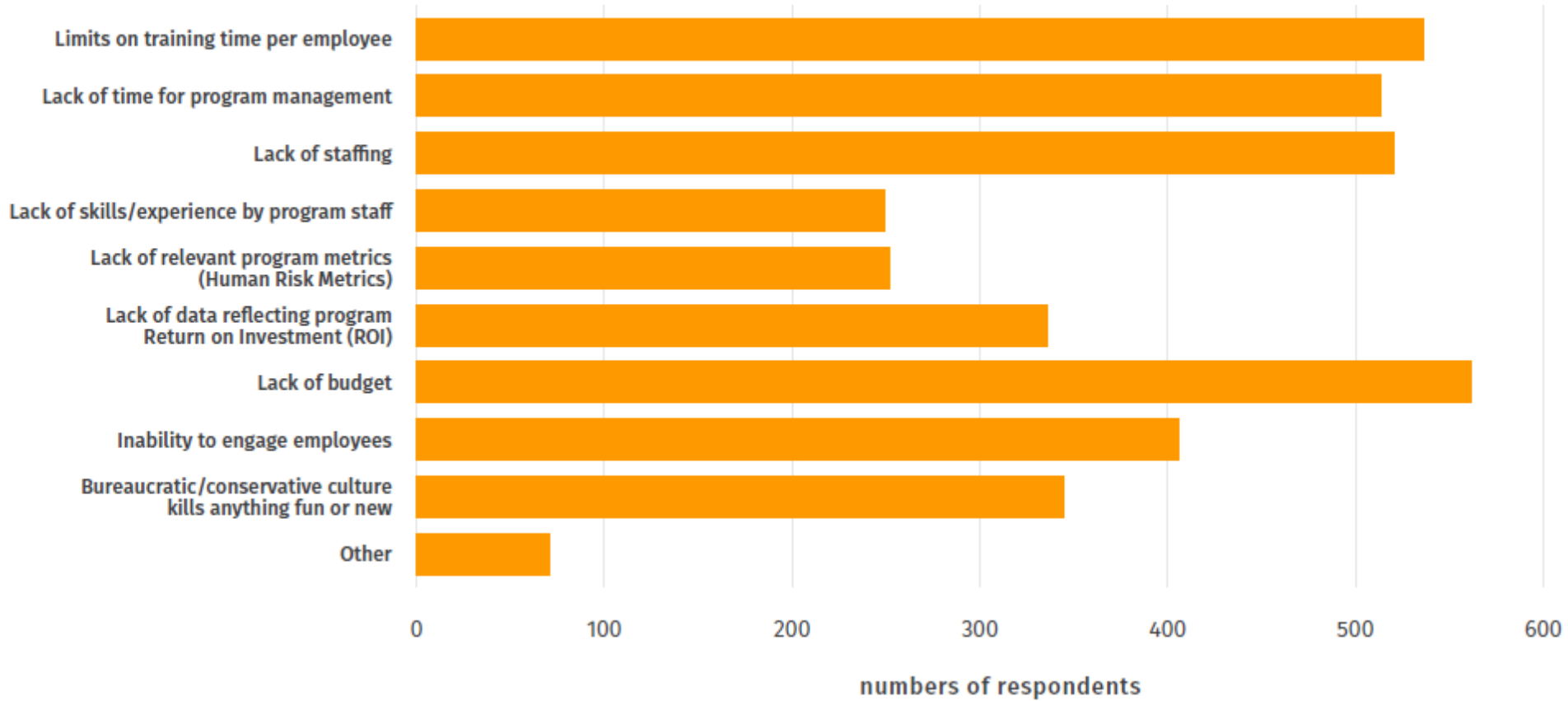


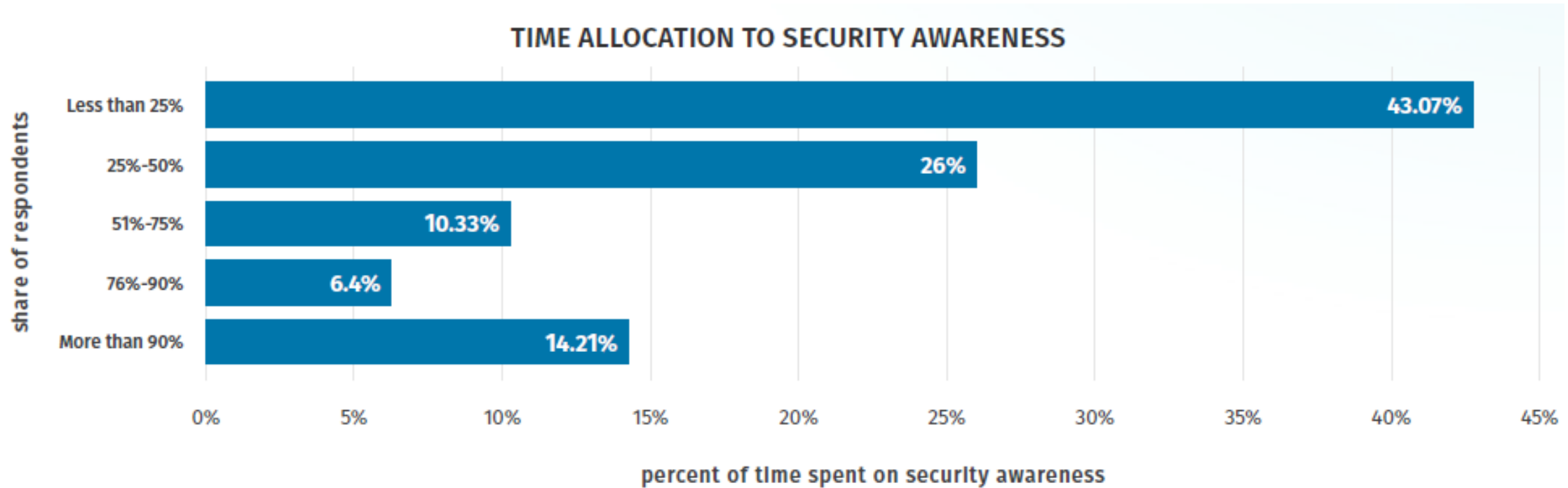


TOP HUMAN RISKS TO ORGANIZATIONS



PROGRAM CHALLENGES





“Security awareness is often perceived by organizations as a part-time task, with almost 70% of security awareness practitioners reporting this year that they spend 50% or less of their time on it.”

PROGRAM MATURITY BY LEADERSHIP SUPPORT

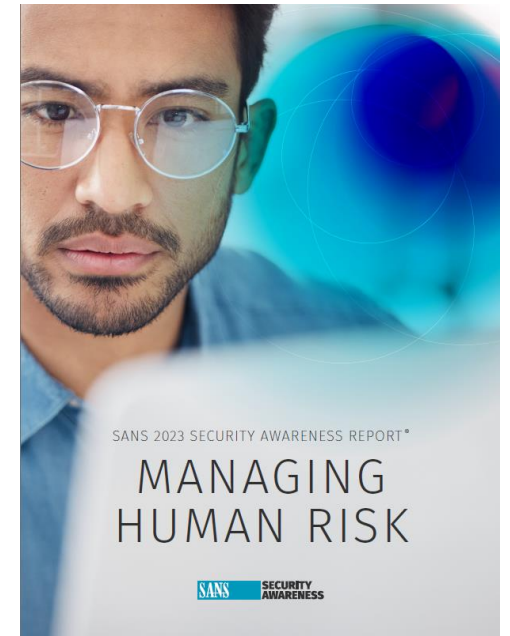
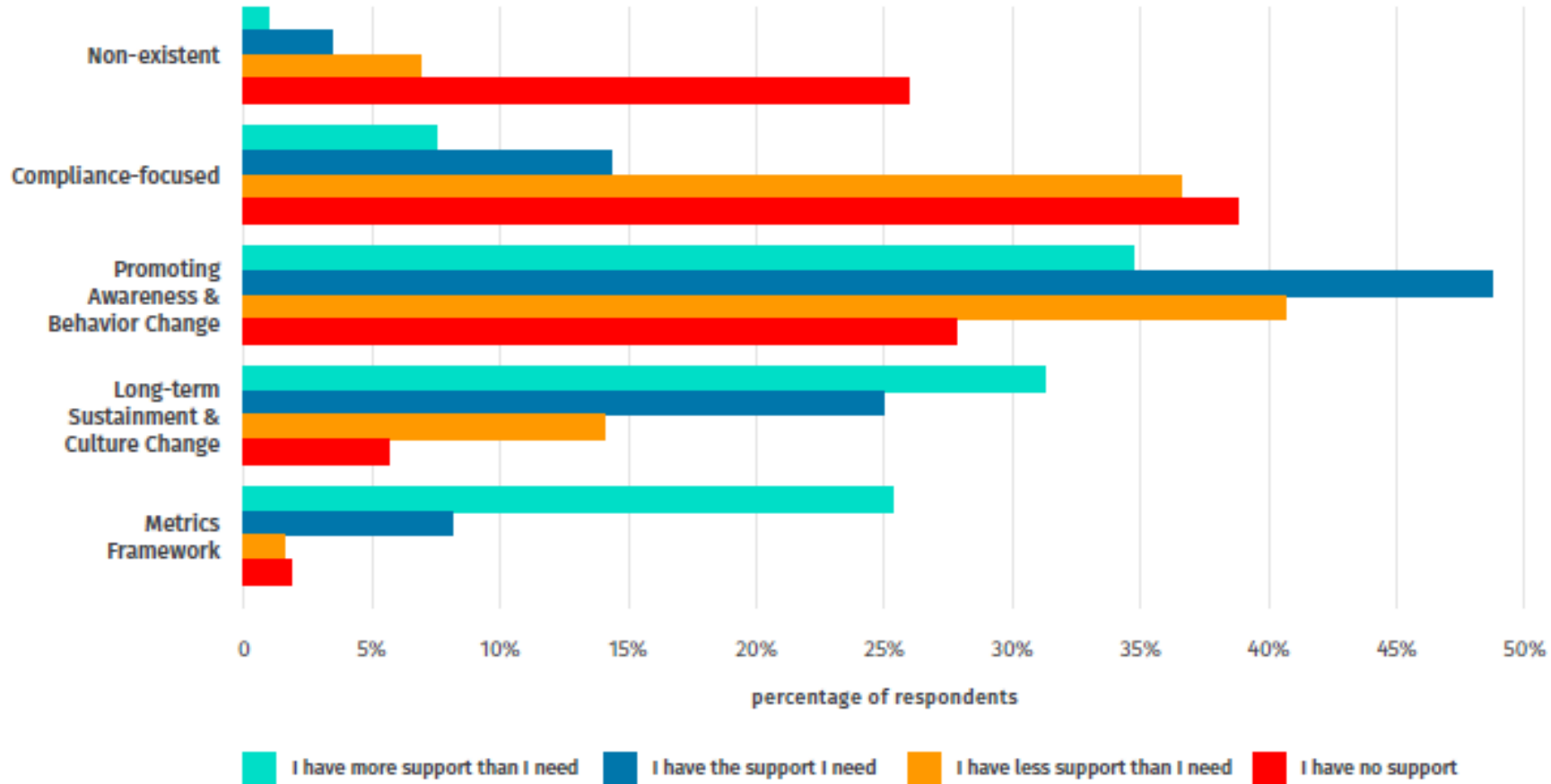


TABLE 3-2: AWARENESS AND TRAINING FAMILY

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



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

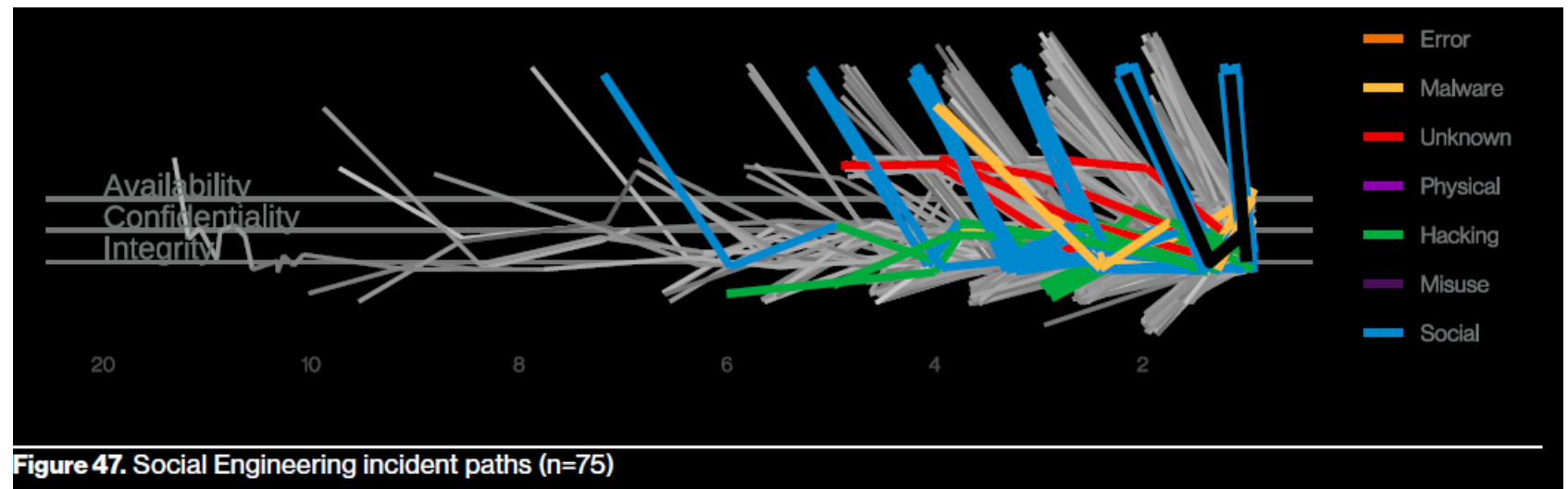
National Institute of Standards and Technology
 Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

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



Social Engineering

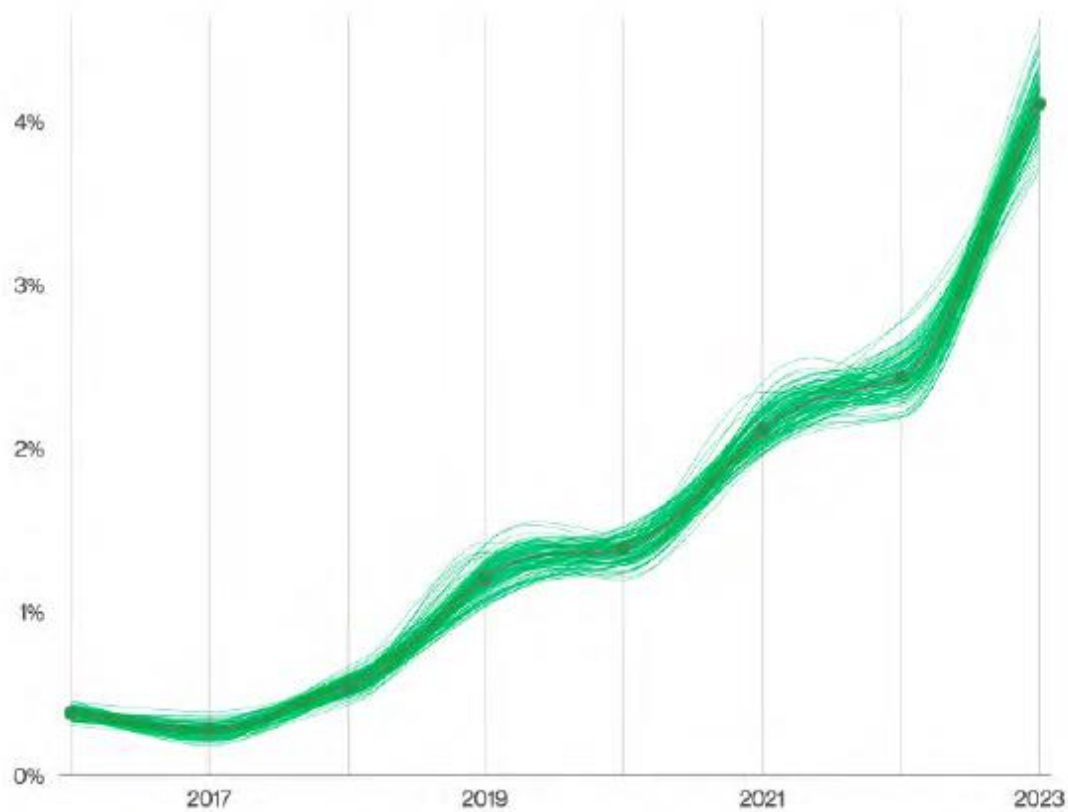


Figure 36. Pretexting incidents over time

Frequency 1,700 incidents, 928 with confirmed data disclosure

Threat actors External (100%), Multiple (2%), Internal (1%), Partner (1%) (breaches)

Actor motives Financial (89%), Espionage (11%) (breaches)

Data compromised Credentials (76%), Internal (28%), Other (27%), Personal (26%) (breaches)

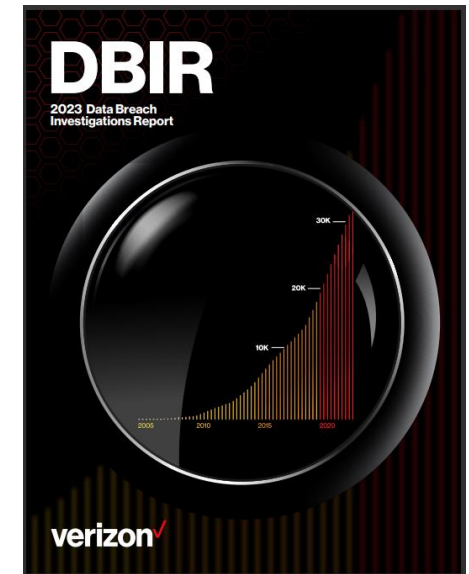
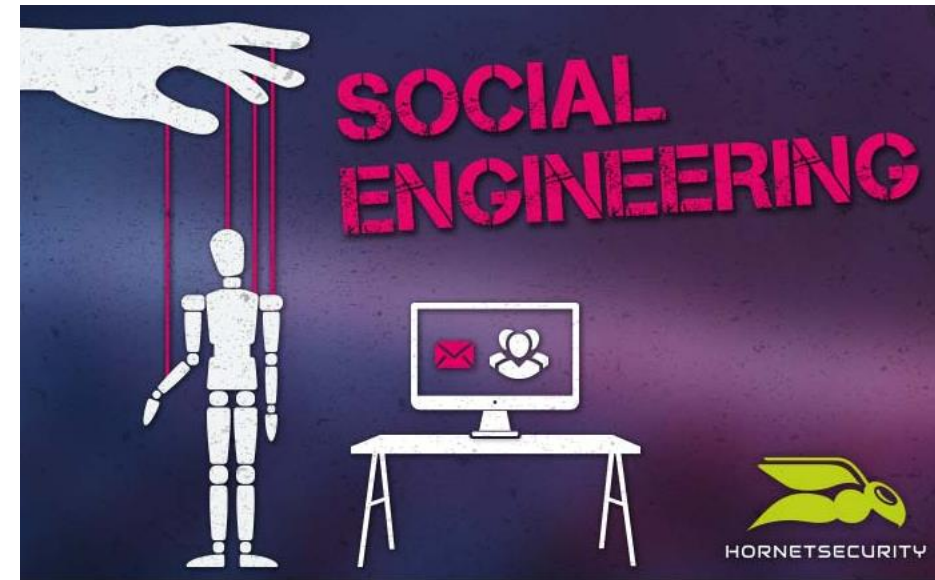


Figure 35. Action varieties in Social Engineering incidents (n=1,696)

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...)

- ▶ 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



“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
- 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 $\frac{1}{4}$ 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
- ✓ Test Taking Tip
- ✓ Quiz

Protecting Information Assets

- Unit# 3a -

Creating a Security Aware Organization