

# Protecting Information Assets

- Unit# 2b -

## 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

---

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

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	<b>Policy and Procedures</b>	X	X	X	X
AT-2	<b>Literacy Training and Awareness</b>	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	<b>Role-Based Training</b>	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	<b>Training Records</b>	X	X	X	X
AT-5	<b>Contacts with Security Groups and Associations</b>	W: Incorporated into PM-15.			
AT-6	<b>Training Feedback</b>				

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?**

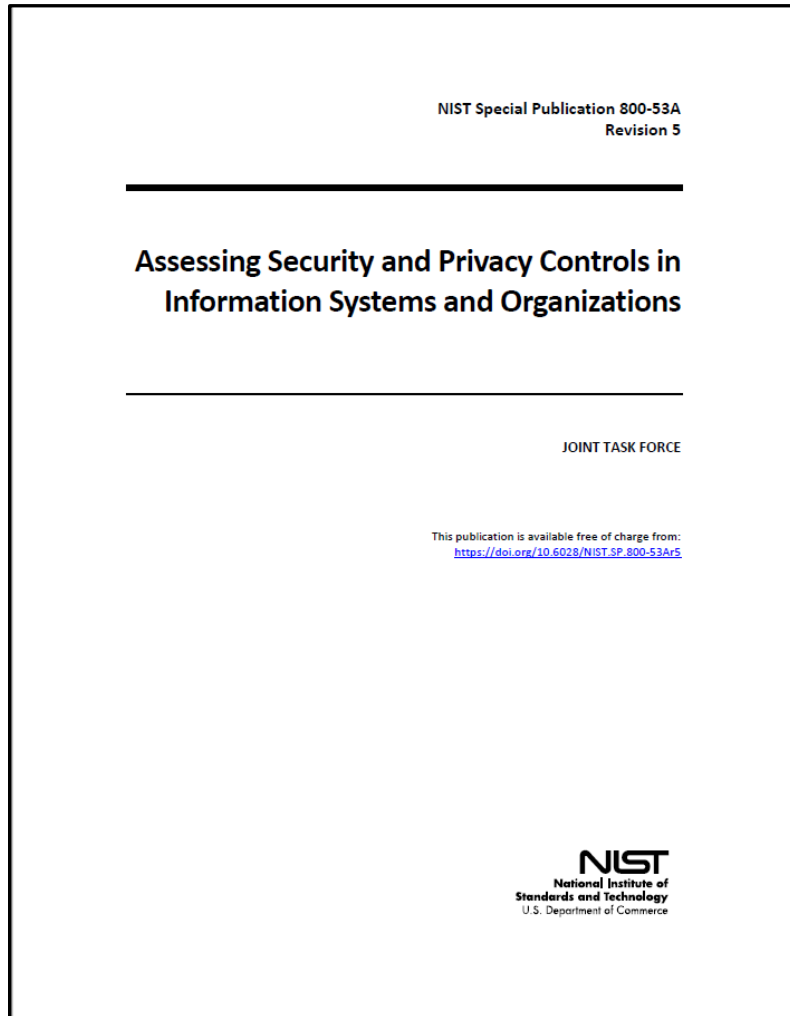
Dataset	Informaton Type	IMPACT RATINGS			
		Confidentiality	Integrity	Availability	Security Categorization
1	Assets and Liability Management	Low	Low	Low	Low
2	Reporting and Information	Low	Moderate	Low	Moderate
3	Funds Control	Moderate	Moderate	Low	Moderate
4	Accounting	Low	Moderate	Low	Moderate
5	Payments	Low	Moderate	Low	Moderate
6	Collecitons and Receivables	Low	Moderate	Low	Moderate
7	Cost Accounting/Performance Measurement	Low	Moderate	Low	Moderate
<b>Overall Categorization:</b>		<b>Moderate</b>	<b>Moderate</b>	<b>Low</b>	<b>Moderate</b>

**The overall security categorization: *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	<b>Policy and Procedures</b>	X	X	X	X
AT-2	<b>Literacy Training and Awareness</b>	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	<b>Role-Based Training</b>	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	<b>Training Records</b>	X	X	X	X
AT-5	Contacts with Security Groups and Associations		W: Incorporated into PM-15.		
AT-6	<b>Training Feedback</b>				



# Exercise:

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

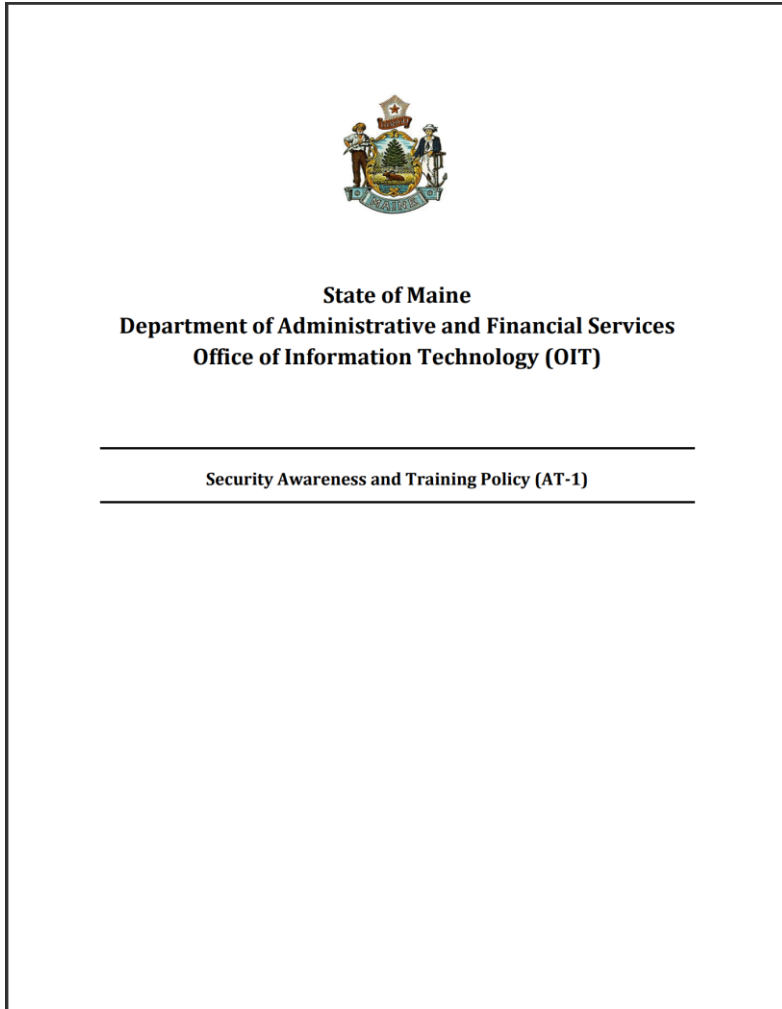


TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
<b>AT-1</b>	<b>Policy and Procedures</b>	X	X	X	X
<b>AT-2</b>	<b>Literacy Training and Awareness</b>	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				
<b>AT-3</b>	<b>Role-Based Training</b>	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			
<b>AT-4</b>	<b>Training Records</b>	X	X	X	X
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
<b>AT-6</b>	<b>Training Feedback</b>				

AT-01 POLICY AND PROCEDURES	
<b>ASSESSMENT OBJECTIVE:</b> <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

**Table of Contents**

- 1.0 Purpose.....3
- 2.0 Scope.....3
- 3.0 Conflict.....3
- 4.0 Roles and Responsibilities.....3
- 5.0 Management Com
- 6.0 Coordination Amo
- 7.0 Compliance.....
- 8.0 Procedures.....
- 9.0 Document Details.
- 10.0 Review.....
- 11.0 Records Managem
- 12.0 Public Rec
- 13.0 Definitions.....
- 14.0 Abbreviations.....

**Security Awareness and Training Policy (AT-1)**

**1.0 Purpose**  
The purpose of this document is to outline the State of Maine's policy and procedures for security awareness and training. This corresponds to the Awareness and Training (AT) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

**2.0 Scope**  
This document applies to all State of Maine Executive Branch personnel, both employees and contractors.

**3.0 Conflict**  
If this document conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

**4.0 Roles and Responsibilities**

4.1 Agency Management

- 4.1.1 Enforces this policy as outlined in section 7.0, Compliance.
- 4.1.2 Establishes and conducts privacy training to meet regulatory requirements and business needs.
- 4.1.3 Ensures that agency personnel have access to and receive the enterprise security awareness training (see Definitions) at required intervals. This includes:
  - 4.1.3.1 Ensuring that agency personnel with access to State email receive the enterprise security awareness training delivered by the Office of Information Technology.
  - 4.1.3.2 Ensuring that agency personnel without access to State email are provided with alternative access to the enterprise security awareness training.
- 4.1.4 Determines agency personnel security awareness training requirements that extend beyond the enterprise security awareness training.
- 4.1.5 Ensures agency personnel are aware of all applicable penalties for noncompliance. (See section 7.0).
- 4.1.6 Maintains agency personnel security awareness training records, in accordance with State of Maine and any additional statutory records retention requirements that apply.
- 4.1.7 Develops and implements agency-level policy and procedures to meet Federal statutory requirements pertinent to security awareness and training.

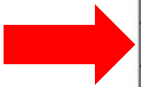
4.2 OIT Information Security Office

- 4.2.1 Owns, executes, and shares responsibility for enforcement of this policy.
- 4.2.2 Determines the training modules and content to be included in enterprise security awareness training.
  - 4.2.2.1 Delivers enterprise security awareness training to agency personnel who have a State email account.
  - 4.2.2.2 Makes records of training delivered available to authorized agency personnel.

Page 3 of 8

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	<b>Policy and Procedures</b>	X	X	X	X
AT-2	<b>Literacy Training and Awareness</b>	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	<b>Role-Based Training</b>	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	<b>Training Records</b>	X	X	X	X
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
AT-6	<b>Training Feedback</b>				



*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

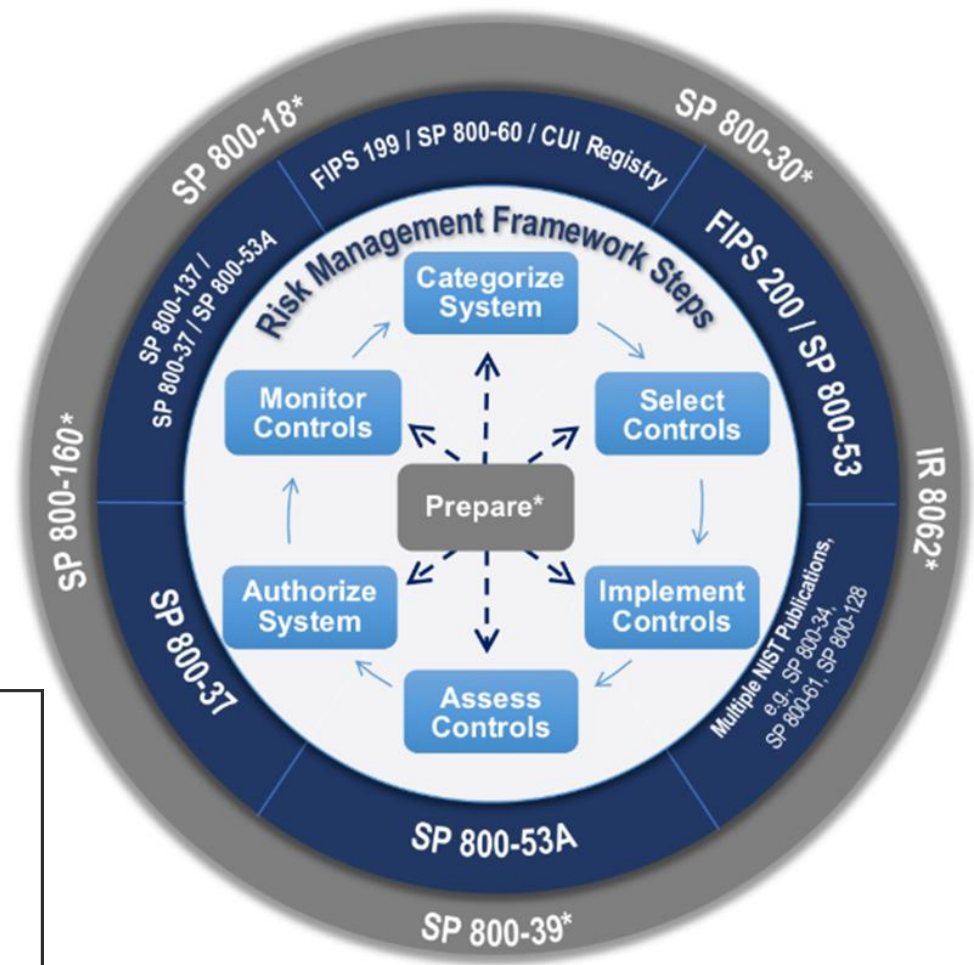
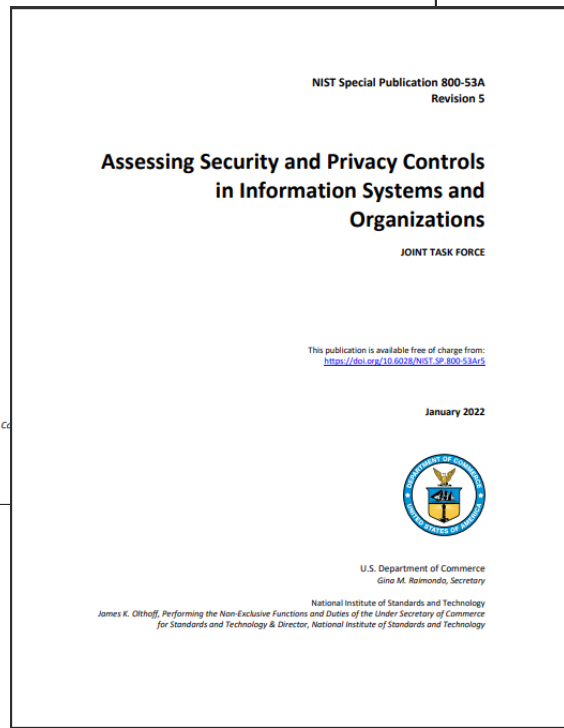
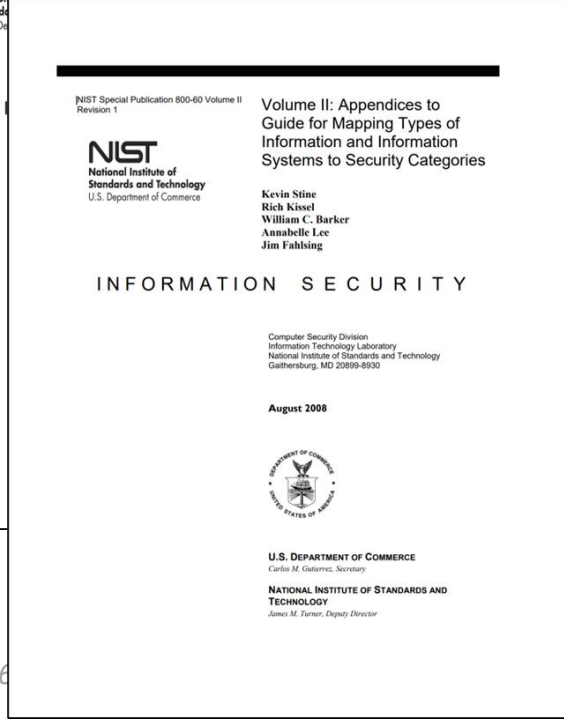
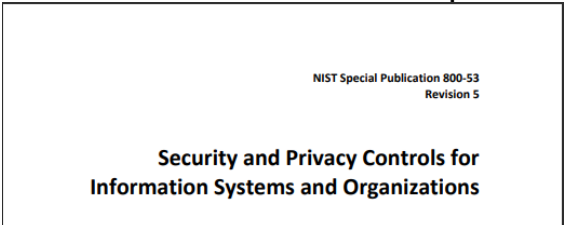
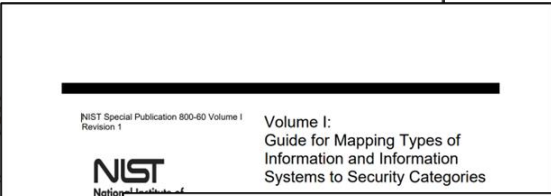
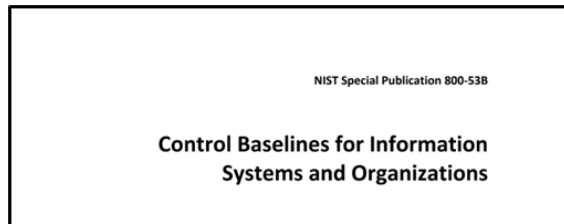
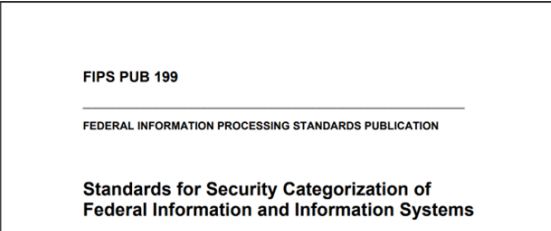
This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-53Ar5>

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

AT-02 LITERACY TRAINING AND AWARENESS	
<b>ASSESSMENT OBJECTIVE:</b> <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;

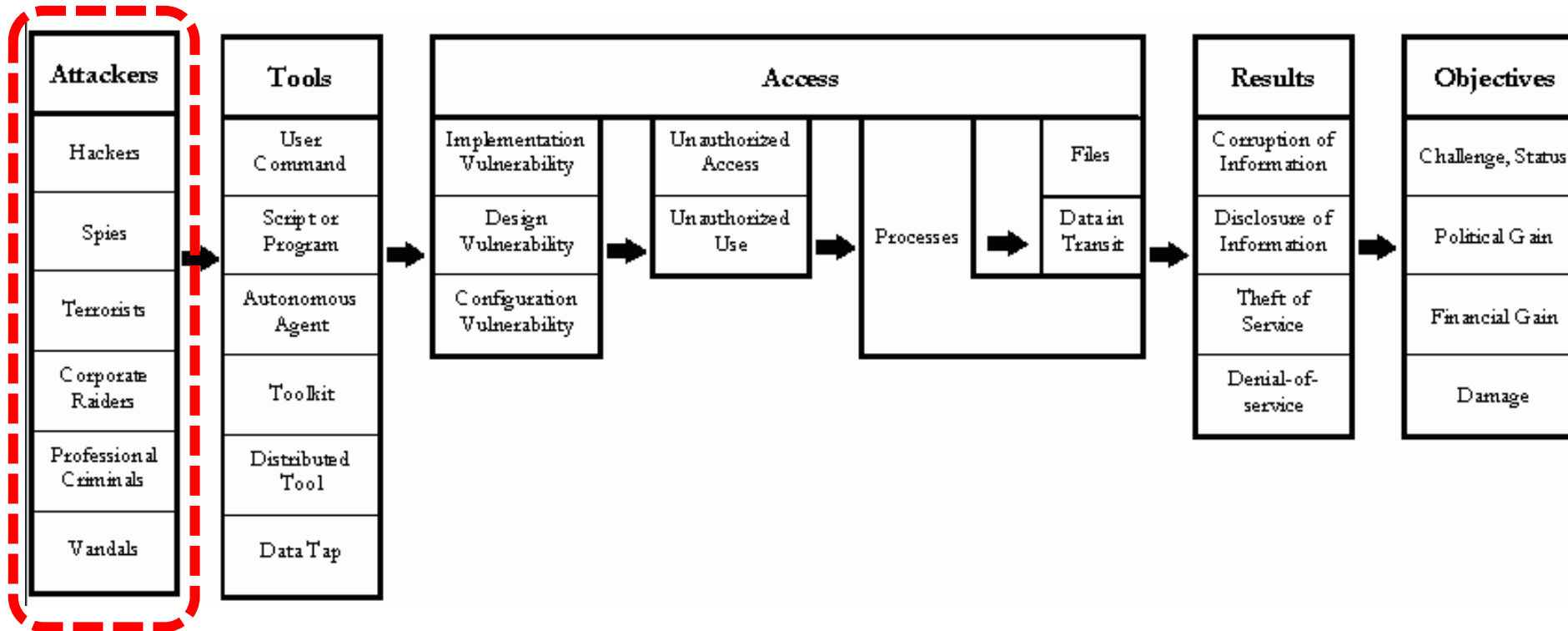
AT-02 LITERACY TRAINING AND AWARENESS	
AT-02a.01[02]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users;
AT-02a.01[03]	security literacy training is provided to system users (including managers, senior 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.
<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b>	
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].

# Let's review



# What is in this picture ?

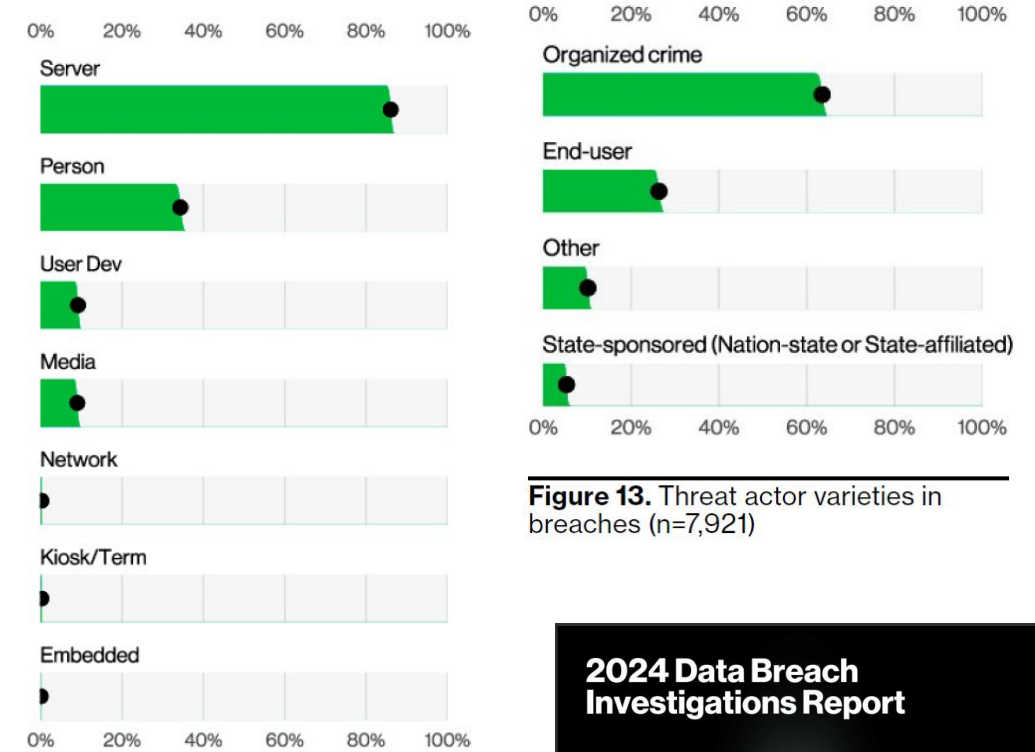
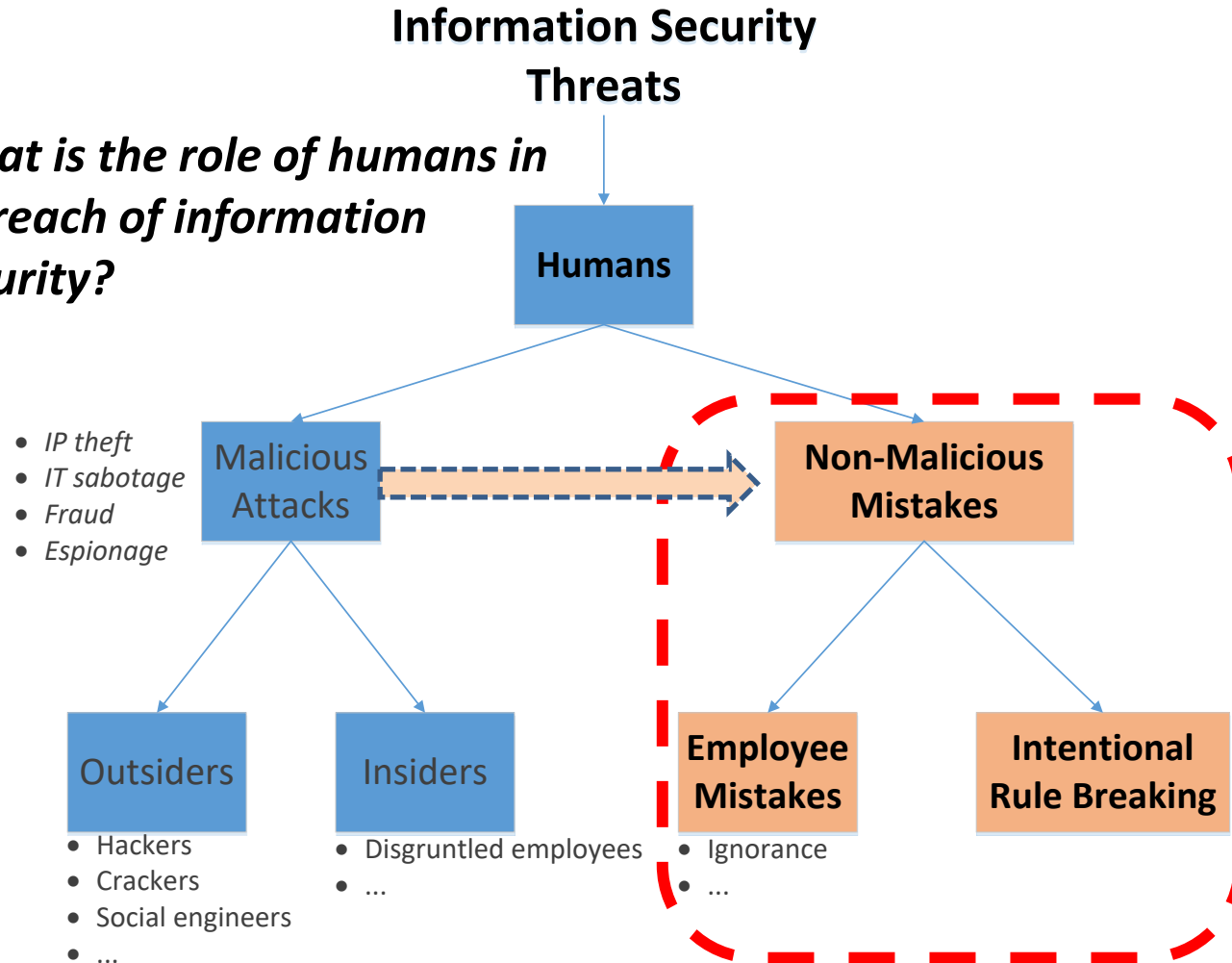
## What is missing from this diagram?



*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 13.** Threat actor varieties in breaches (n=7,921)

**Figure 21.** Assets in breaches (n=8,910)



# What roles do employees play in these attack chains

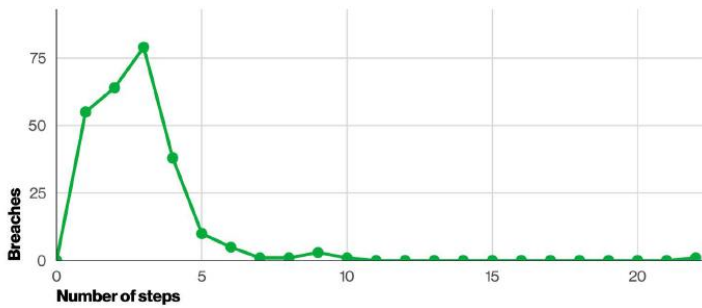
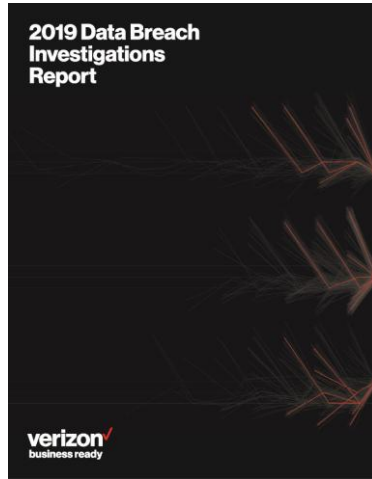


Figure 30. Number of steps per breach in non-Error breaches (n=258)

MIS 5206 Protecting Information Assets

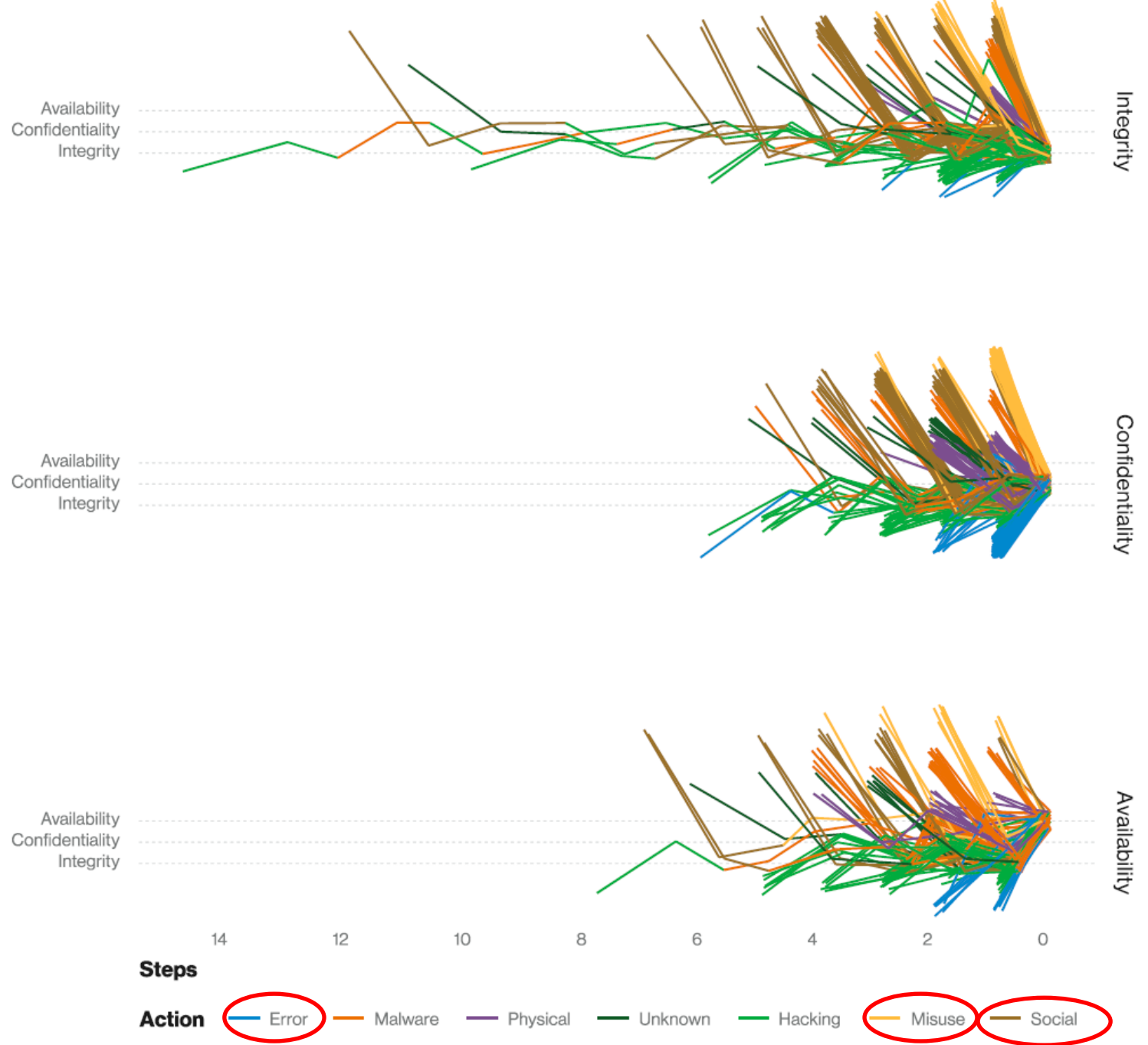


Figure 30. Attack chain by final attribute compromised<sup>12</sup> (n=941)

Figure 1: ENISA Threat Landscape 2024 - Prime threats



*In which of these threats are humans the vulnerability?*

# Patterns over time in breaches



Employee risk areas...

<b>Basic Web Application Attacks</b>	These attacks are against a Web application, and after the initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.
<b>Denial of Service</b>	These attacks are intended to compromise the availability of networks and systems. This includes both network and application layer attacks.
<b>Lost and Stolen Assets</b>	Incidents where an information asset went missing, whether through misplacement or malice, are grouped into this pattern.
<b>Miscellaneous Errors</b>	Incidents where unintentional actions directly compromised a security attribute of an information asset are found in this pattern. This does not include lost devices, which are grouped with theft instead.
<b>Privilege Misuse</b>	These incidents are predominantly driven by unapproved or malicious use of legitimate privileges.
<b>Social Engineering</b>	This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.
<b>System Intrusion</b>	These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying Ransomware.
<b>Everything Else</b>	This "pattern" isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns. Like that container where you keep all the cables for electronics you don't own anymore—just in case.

Table 2. Incident Classification Patterns

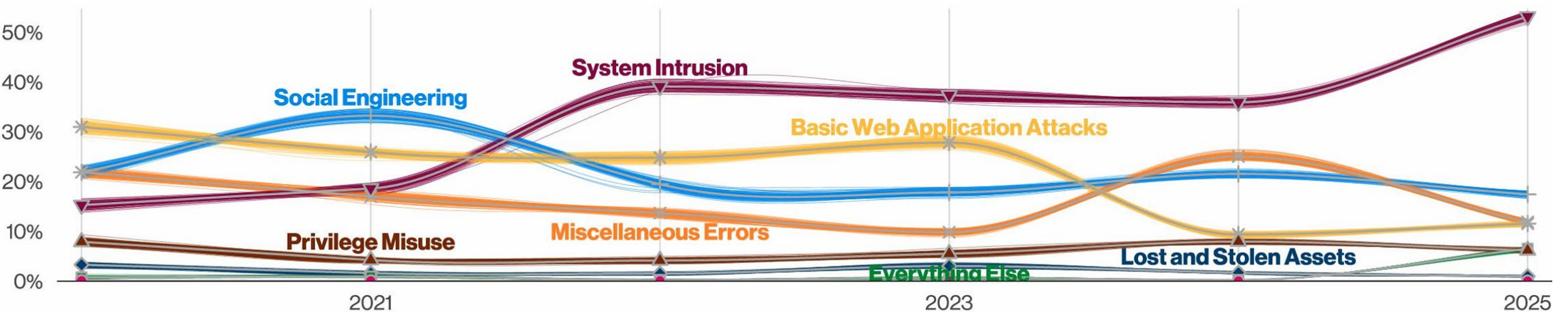
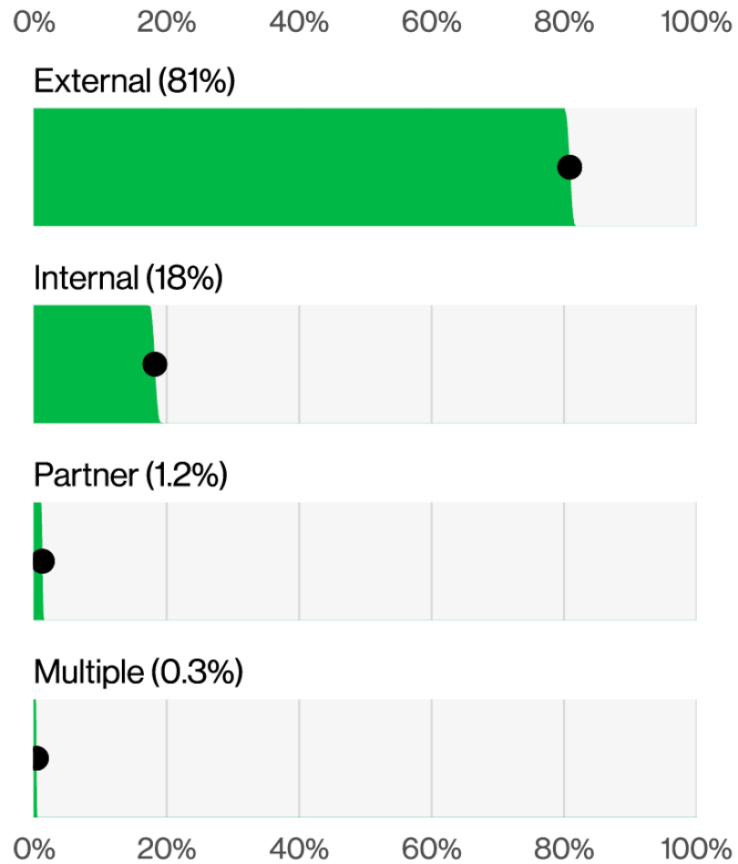
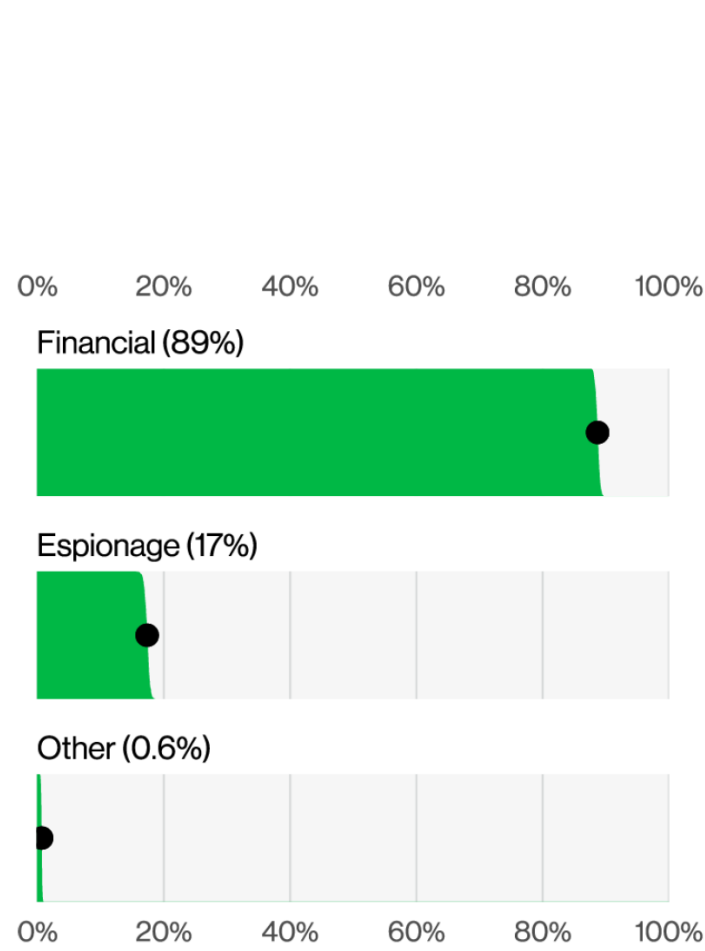


Figure 44. Patterns over time in breaches (n for 2025 dataset=12,195)

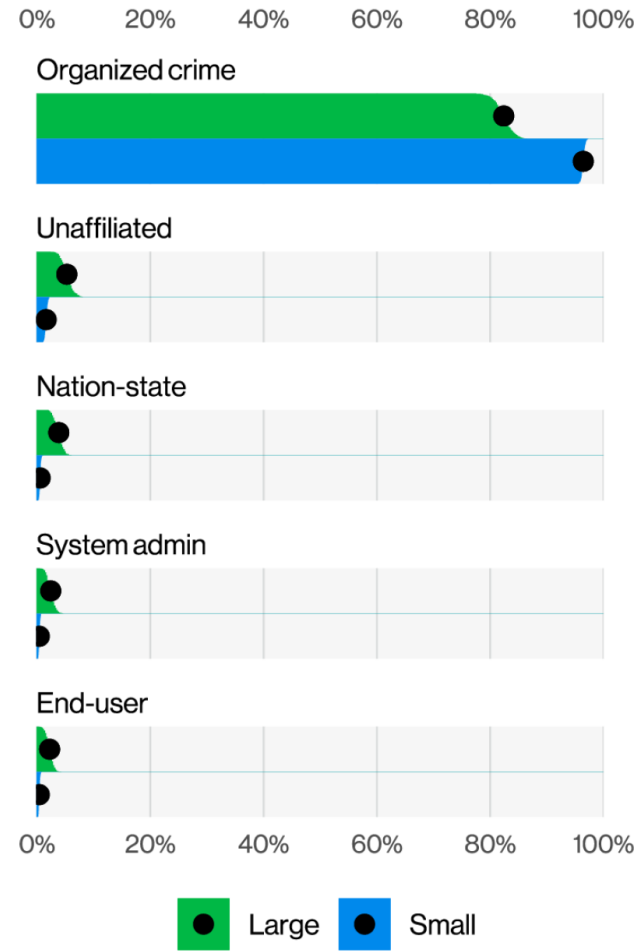
# Threat actors in breaches



**Figure 18.** Threat actors in breaches (n=12,063)

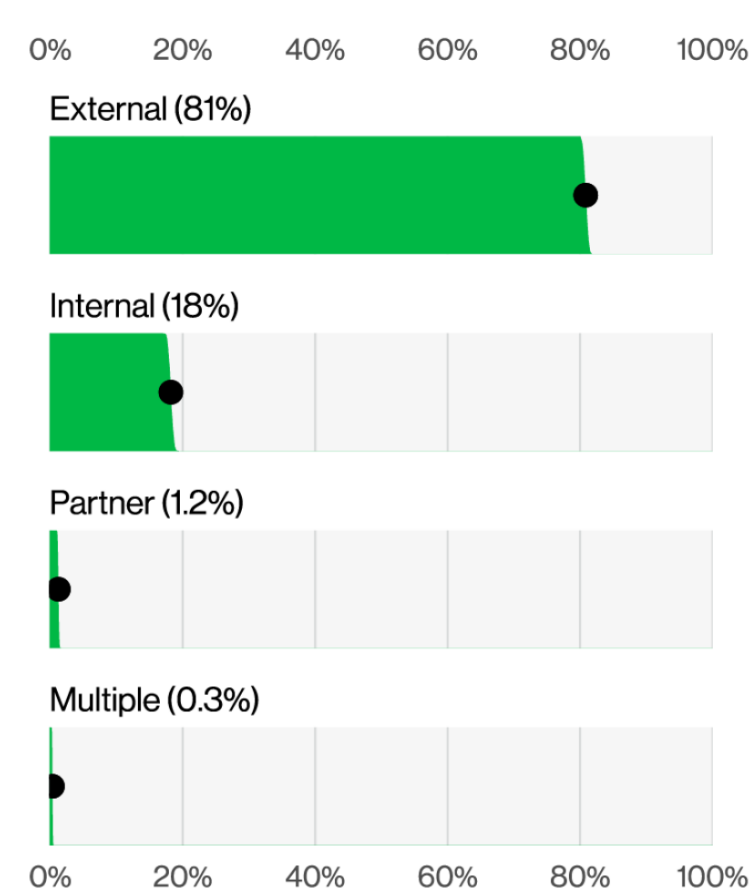


**Figure 21.** Threat actor motives in breaches (n=8,045)

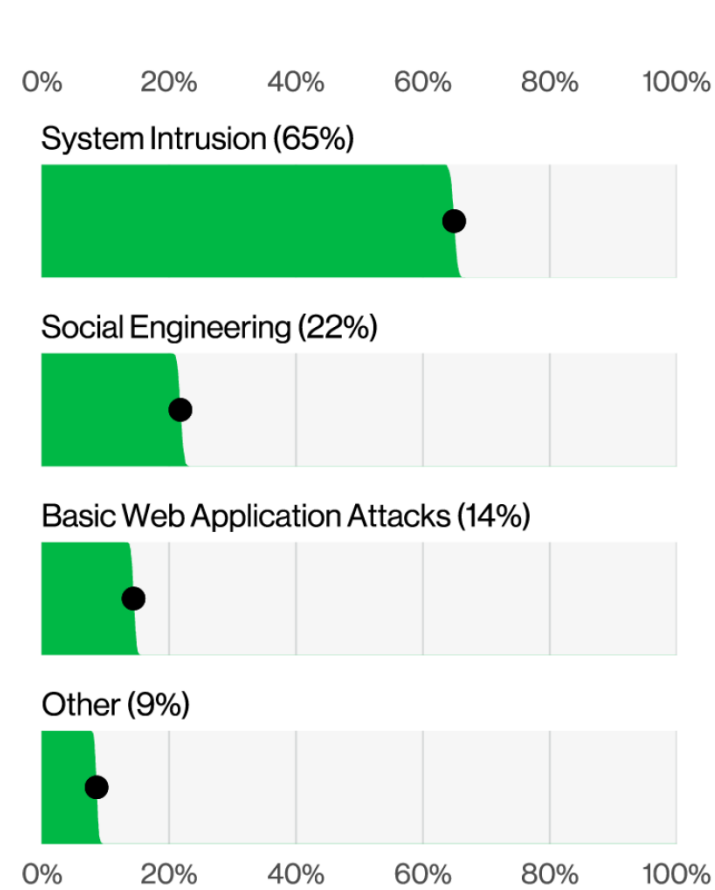


**Figure 91.** Top Actor varieties by victim organization size (n=494)

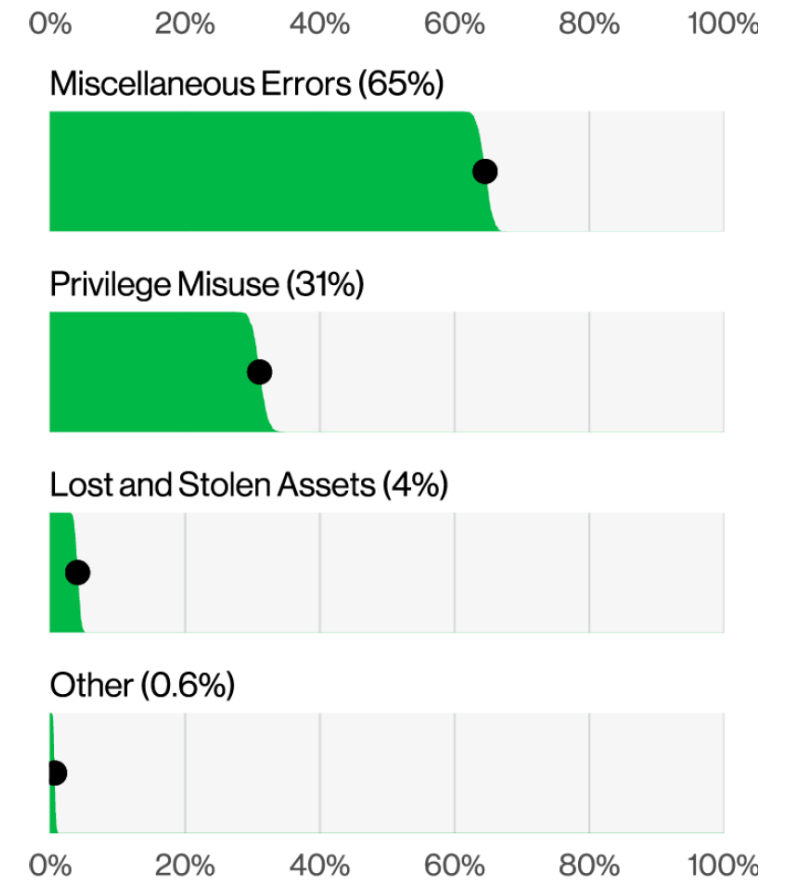
# Patterns in breaches



**Figure 18.** Threat actors in breaches (n=12,063)



**Figure 19.** Patterns in External actor breaches (n=9,754)



**Figure 20.** Patterns in Internal actor breaches (n=2,199)

# 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
  - Training and testing employees
  - Taking advantage of the security options to automate controls
  - Implementing automated checks to assess and 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.”*

# 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...”

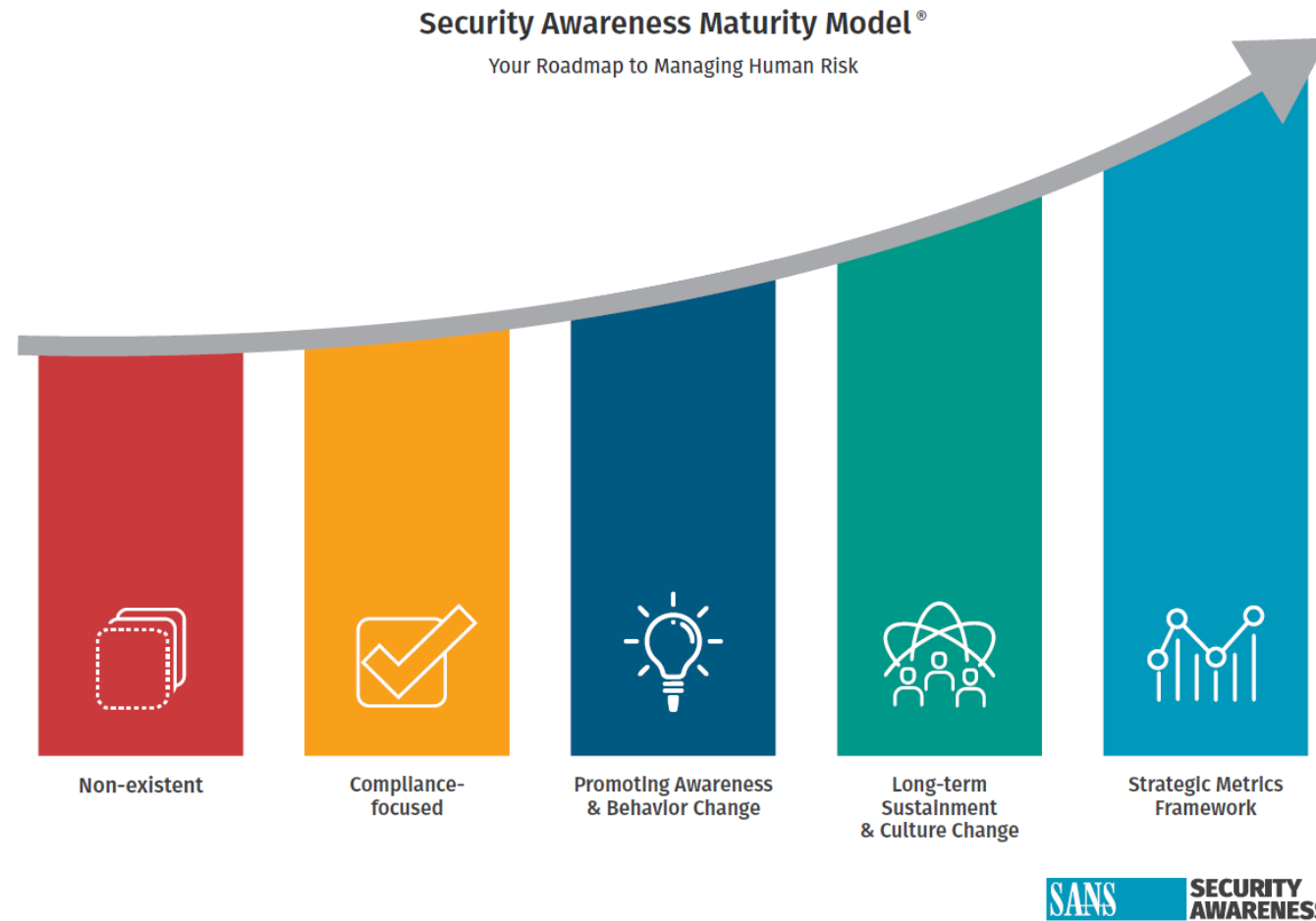
# Auditing a Security Awareness Training control enhancement

AT-2(2)	SECURITY AWARENESS TRAINING   <i>INSIDER THREAT</i>
	<p><b>ASSESSMENT OBJECTIVE:</b></p> <p><i>Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.</i></p>
	<p><b>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</b></p> <p><b>Examine:</b> [<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><b>Interview:</b> [<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				

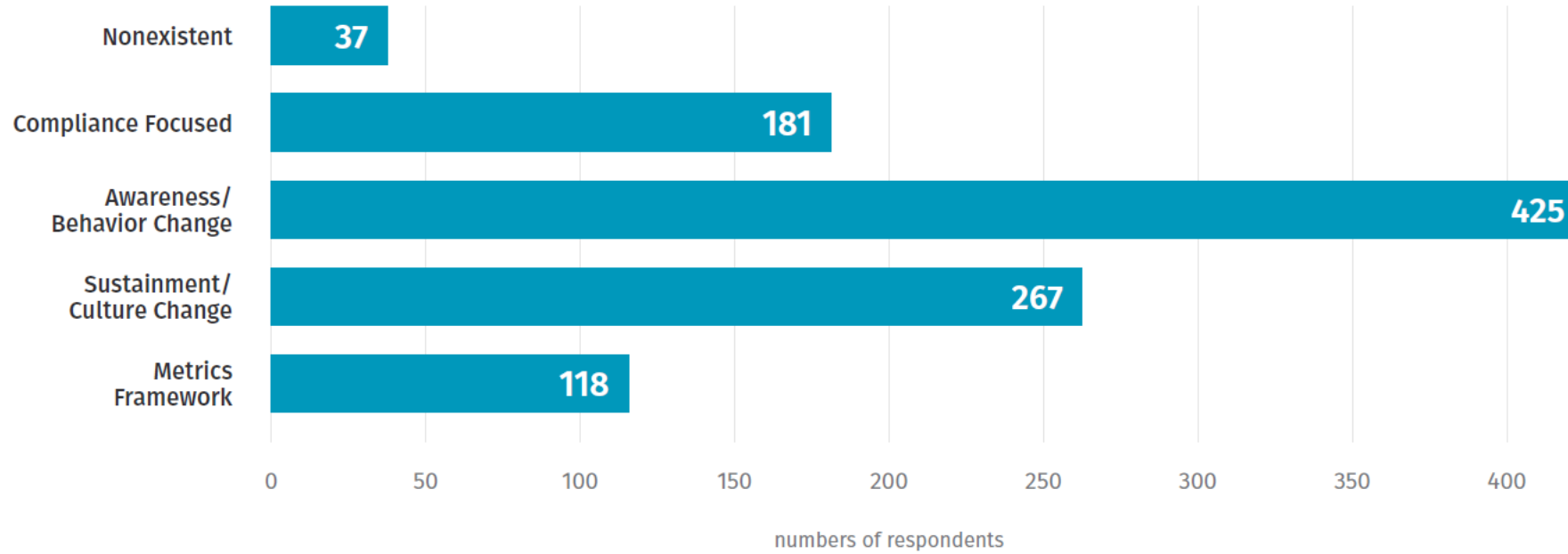
# What phases of security awareness do organizations go through as their programs mature?



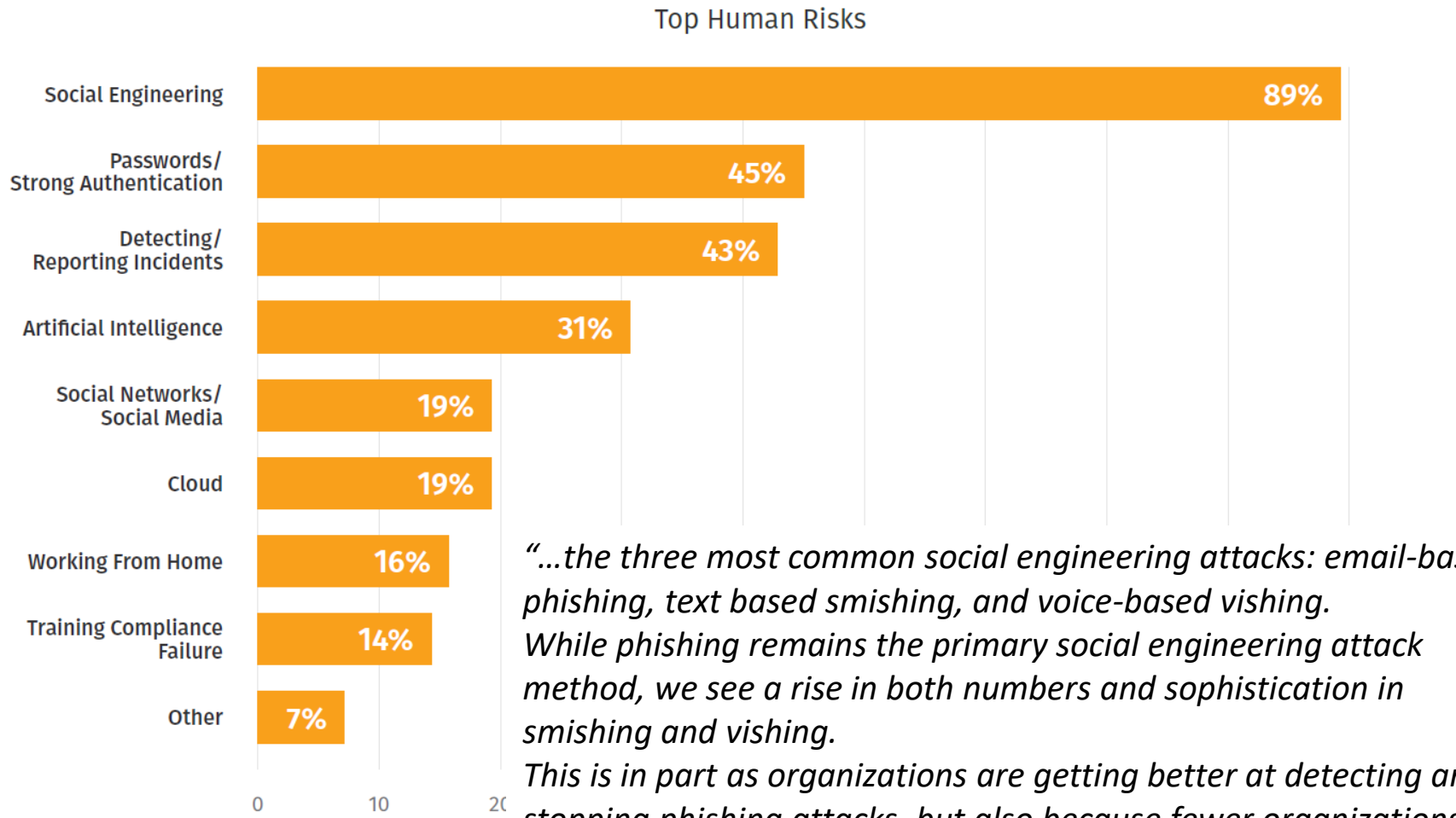
<https://www.sans.org/mlp/ssa-2024-security-awareness-report/>



### Security Awareness Program Maturity Levels



## Top Human Risks: What are the top three concerns or human risks you are focusing on for 2024?



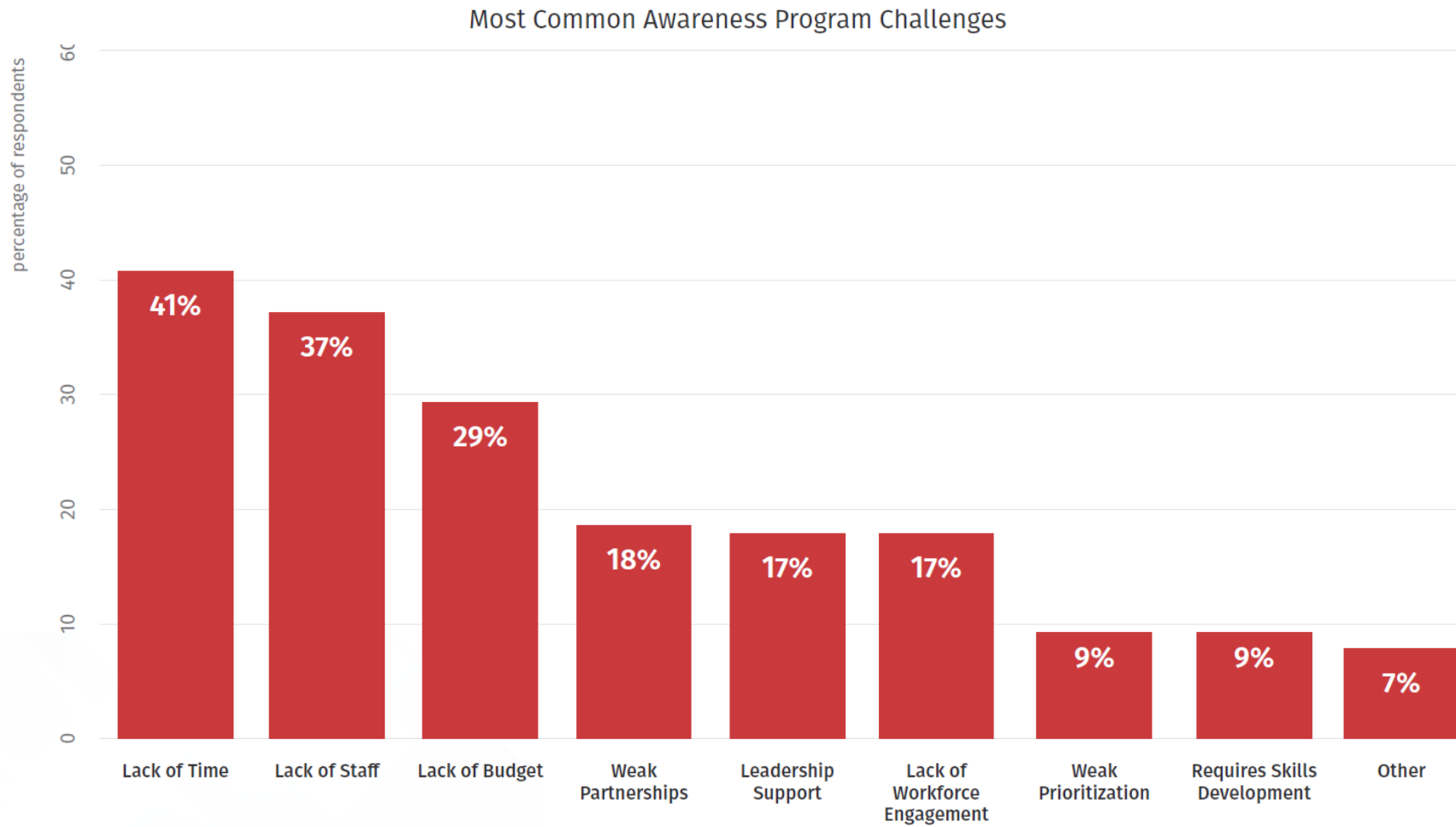
*"...the three most common social engineering attacks: email-based phishing, text based smishing, and voice-based vishing. While phishing remains the primary social engineering attack method, we see a rise in both numbers and sophistication in smishing and vishing.*

*This is in part as organizations are getting better at detecting and stopping phishing attacks, but also because fewer organizations have control over and visibility into employees' mobile devices."*

*Page 9*

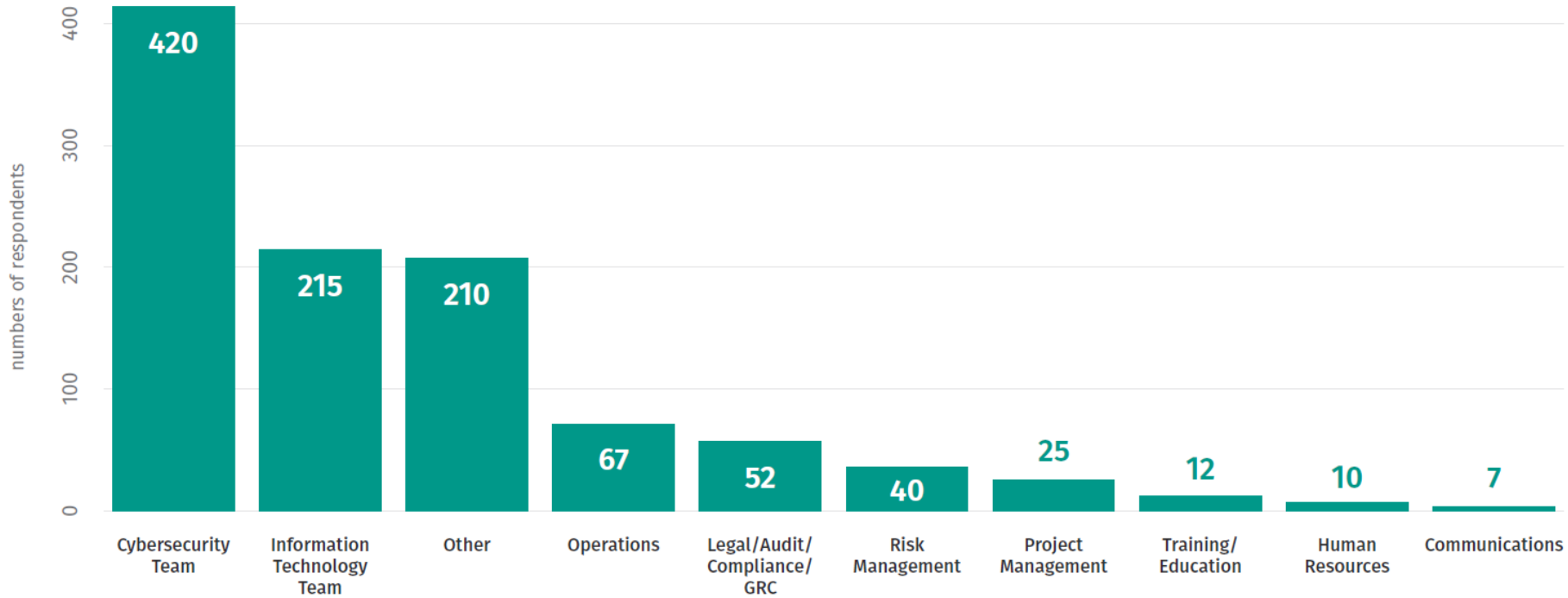


## Program Challenges: What do you feel are the two biggest challenges limiting your ability to succeed?

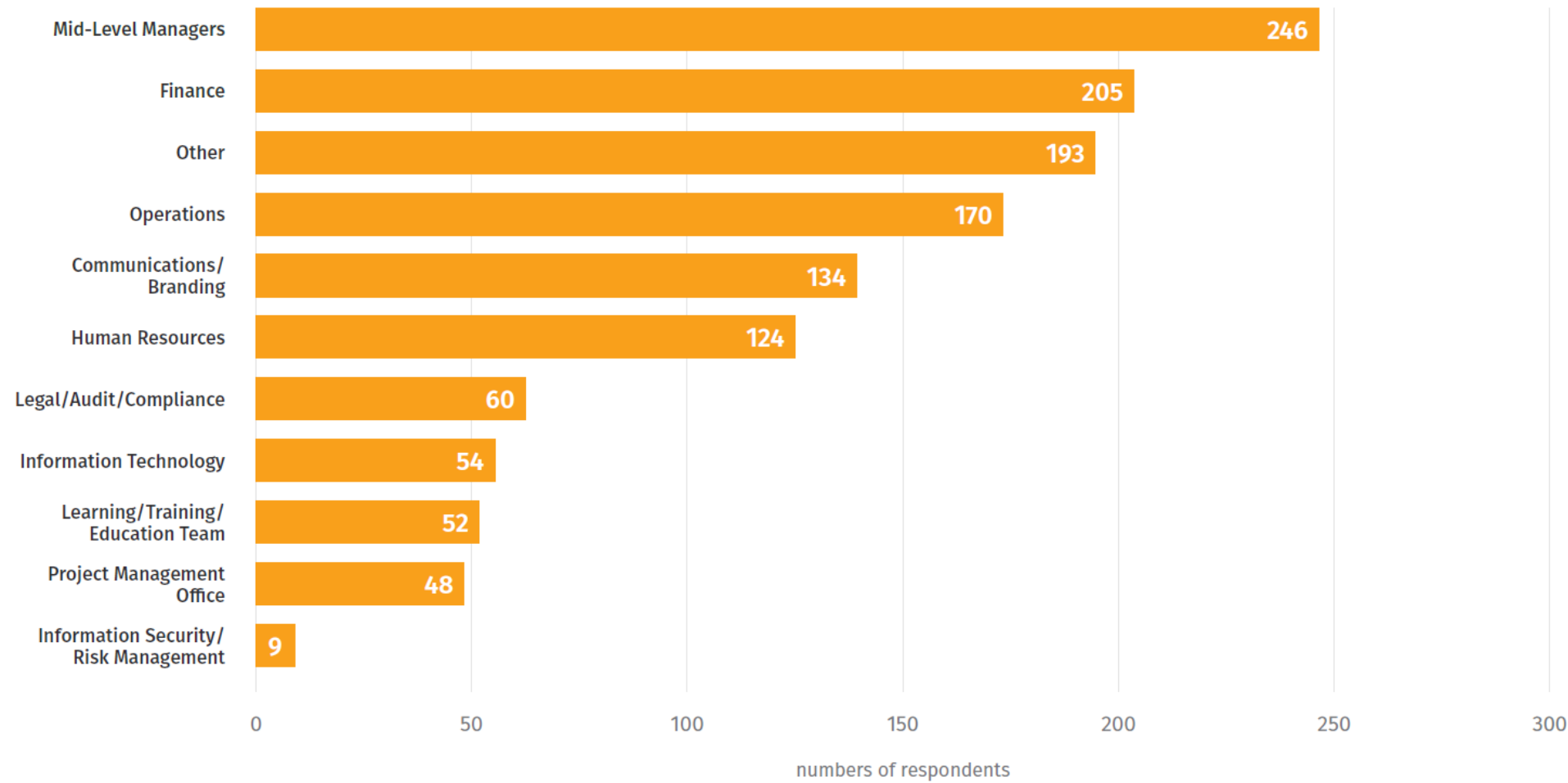


## Reporting: What department best describes where you report to?

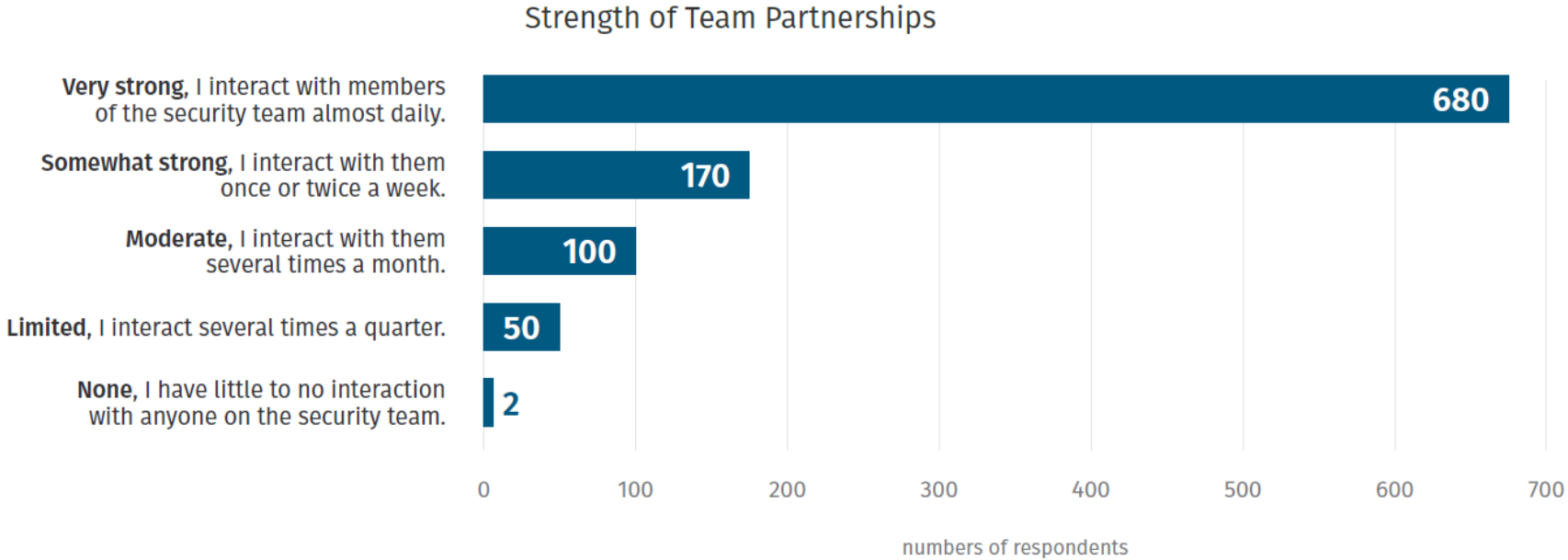
Top Ten Departments the Security Awareness Team Reports



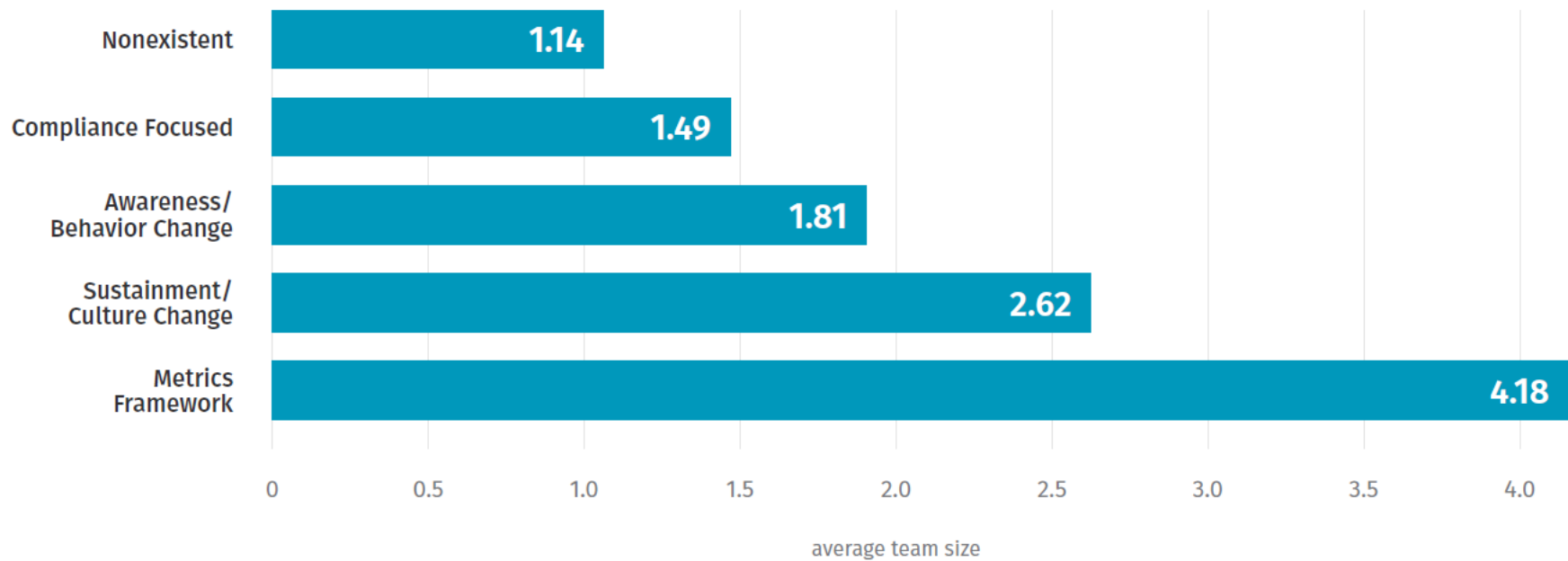
## Security Awareness Program Blockers



**Security Team: How strong is your relationship with the information security team?  
Do you actively partner with them on understanding threats, identifying human risks,  
helping with outbound communications, or interacting with the workforce?**

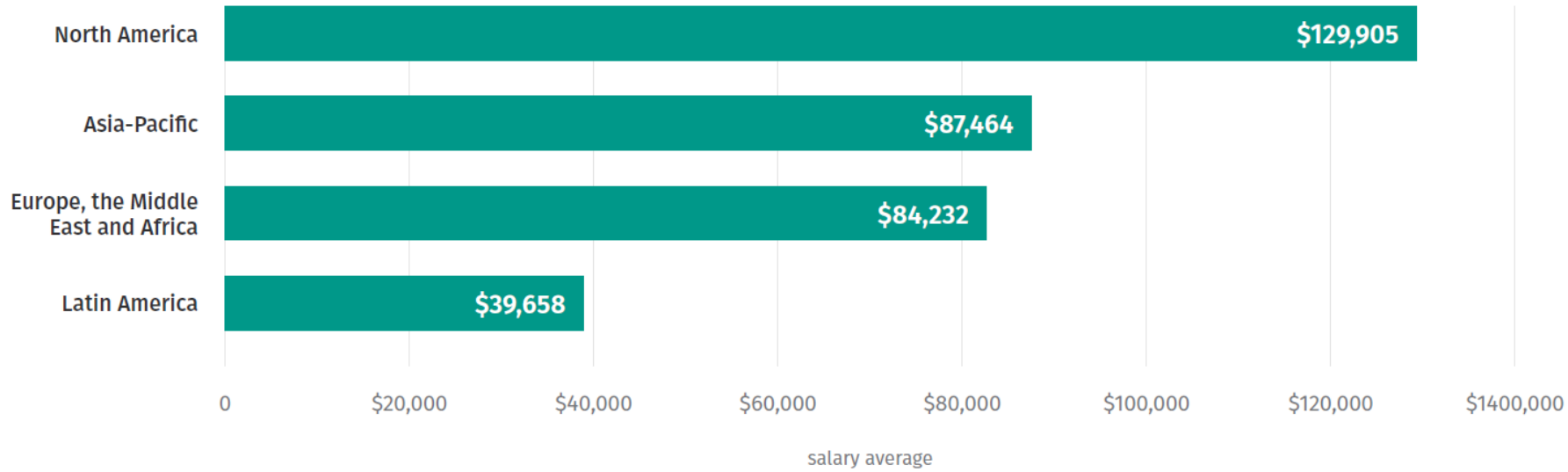


### Average of Full-Time Security Awareness Team Size

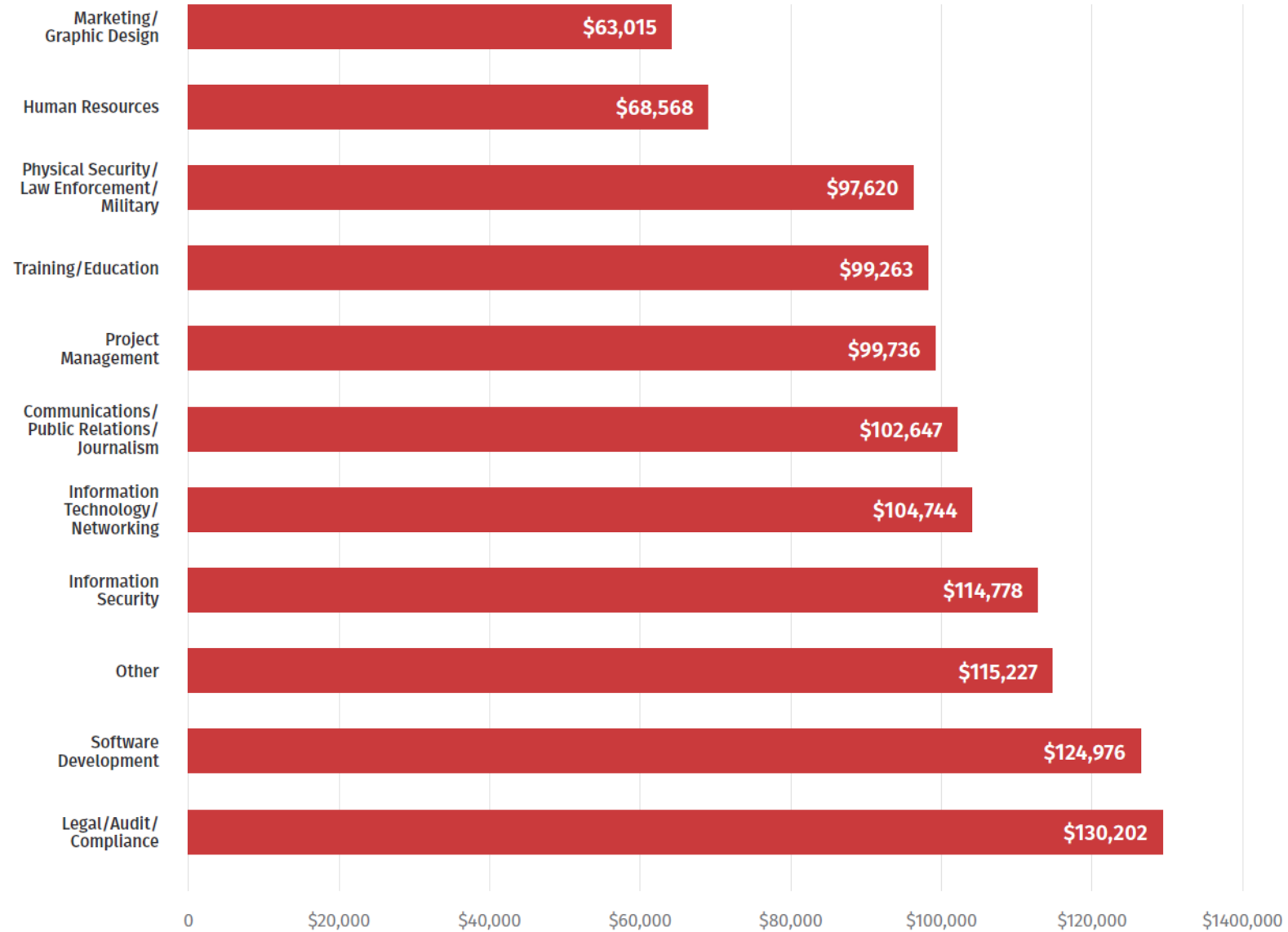


# Average Salaries for Security Awareness Practitioners

Average Salary by Region

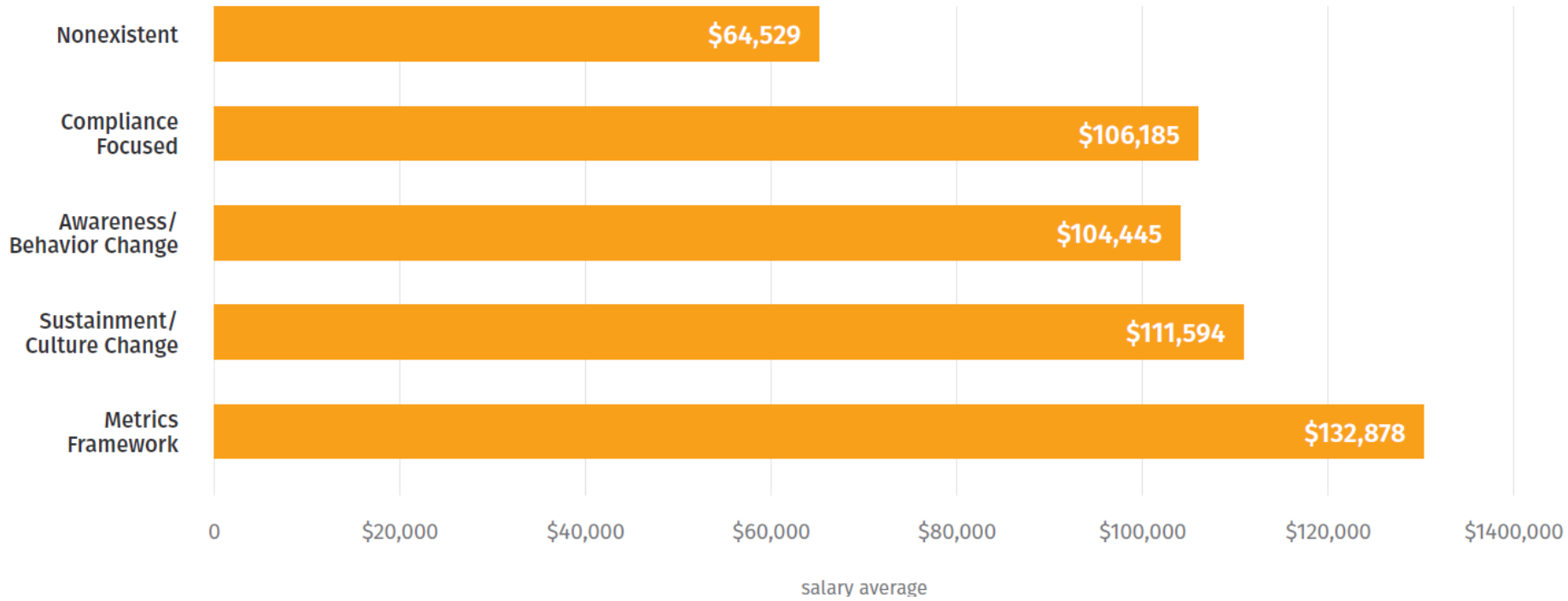


### Average Salary by Professional Background



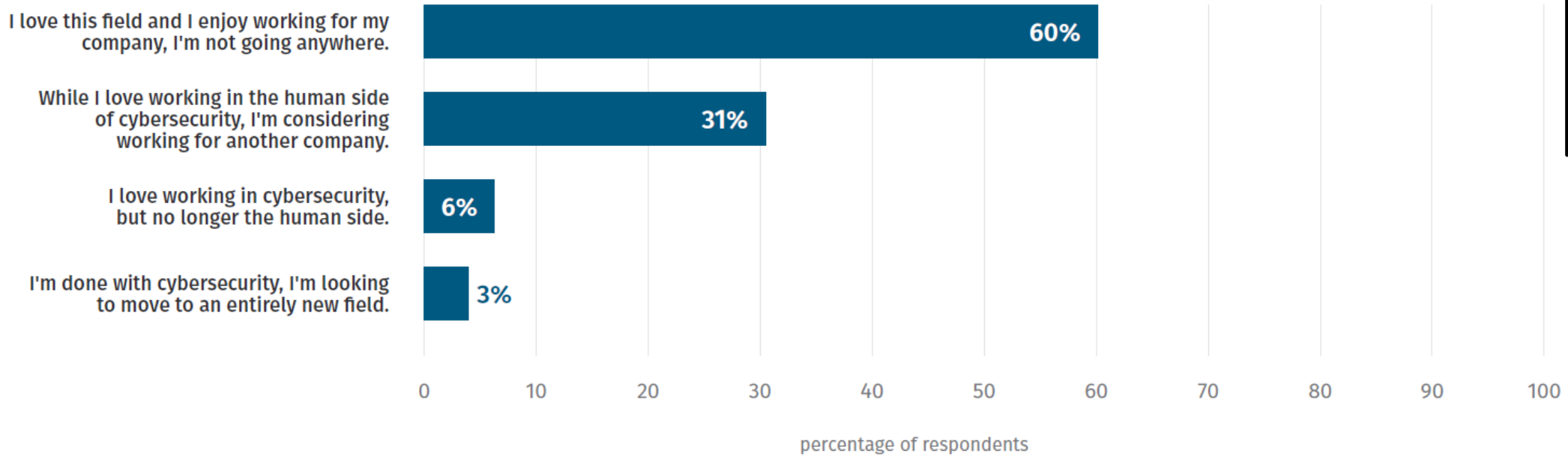
# Average Salaries for Security Awareness Practitioners

Average Salary by Program Maturity

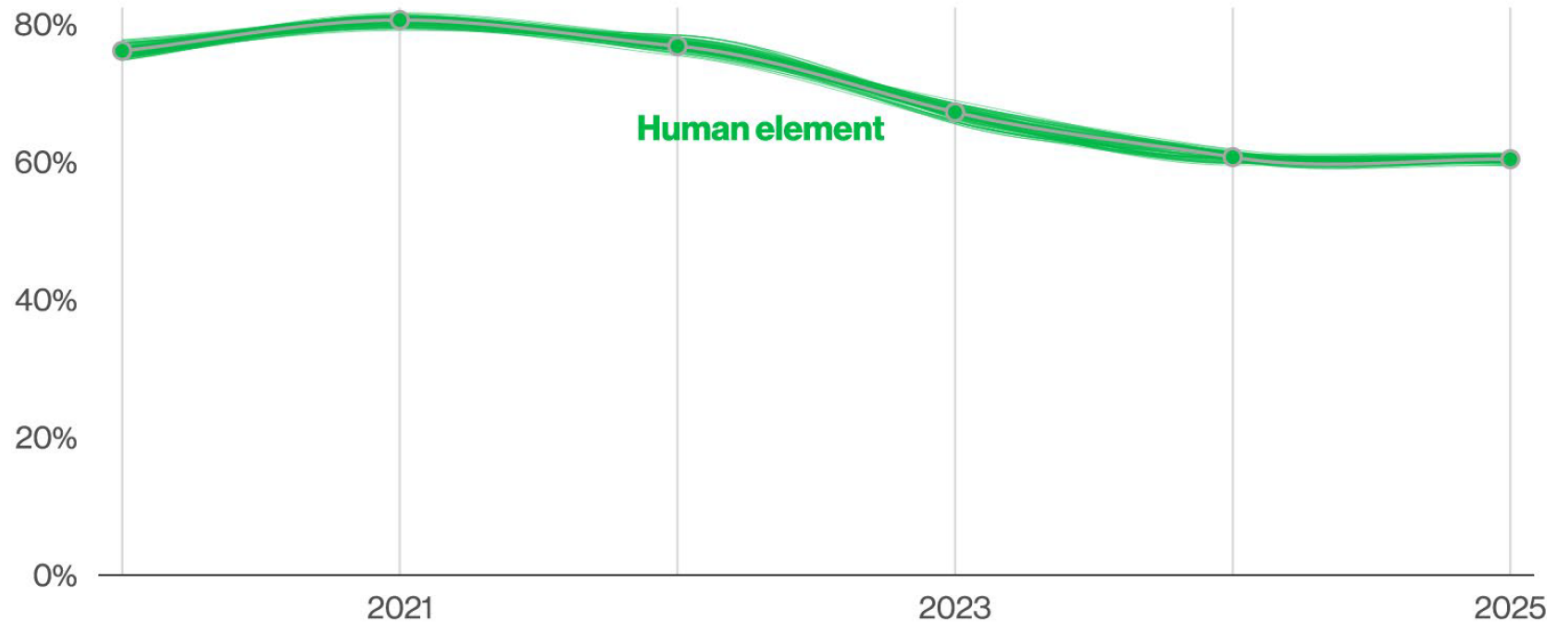


# How Are You Feeling?

## Security Awareness Professionals' Job Satisfaction

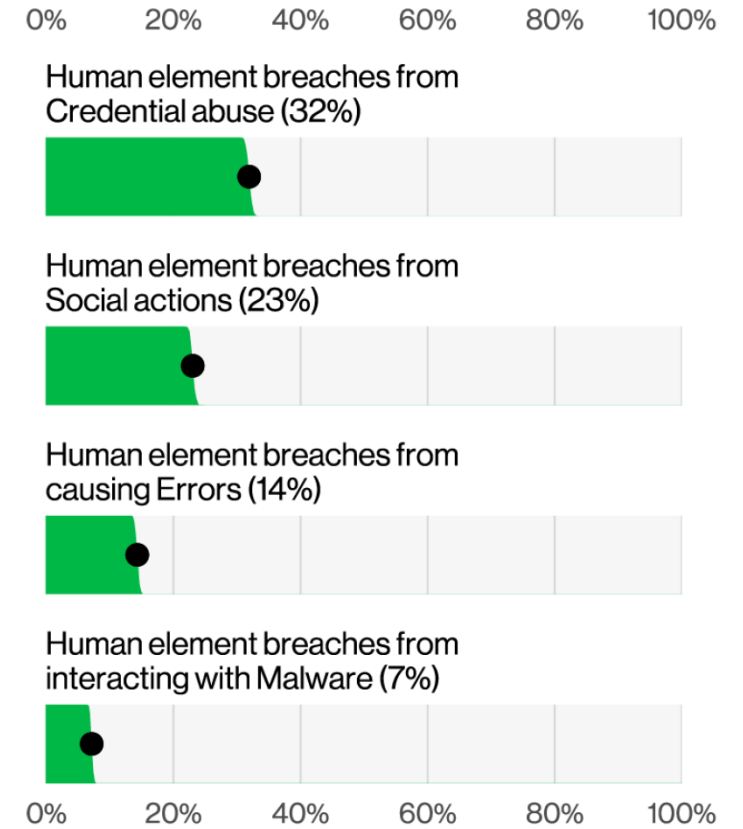


# Human element in breaches



**Figure 14.** Human element involvement over time in breaches

- Humans are a key driver of 60% of breaches (Verizon 2025 DBIR, page 20),
- This is why having a strong security awareness program is important



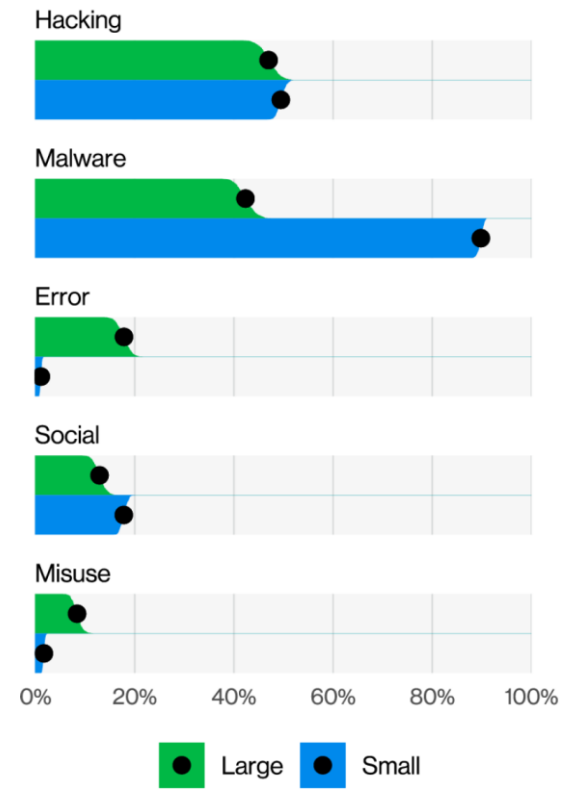
**Figure 15.** Select human element component enumerations in breaches (n=10,798)

**TABLE 3-2: AWARENESS AND TRAINING FAMILY**

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
<b>AT-1</b>	<b>Policy and Procedures</b>	X	X	X	X
<b>AT-2</b>	<b>Literacy Training and Awareness</b>	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				
<b>AT-3</b>	<b>Role-Based Training</b>	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			
<b>AT-4</b>	<b>Training Records</b>	X	X	X	X
AT-5	Contacts with Security Groups and Associations	W: Incorporated into PM-15.			
<b>AT-6</b>	<b>Training Feedback</b>				



Organization size	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
Small businesses (fewer than 1,000 employees)	3,049 incidents, 2,842 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 96% of breaches	External (98%), Internal (2%), Partner (1%) (breaches)	Financial (99%) (breaches)	Internal (83%), Credentials (34%), Other (6%), Personal (4%) (breaches)
Large businesses (more than 1,000 employees)	982 incidents, 751 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 79% of breaches	External (75%), Internal (25%), Partner (1%), Multiple (1%) (breaches)	Financial (95%), Espionage (3%), Ideology (1%) (breaches)	Personal (50%), Other (36%), Credentials (29%), Internal (29%) (breaches)



**Figure 90.** Top Actions by victim organization size (n=751)



# 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

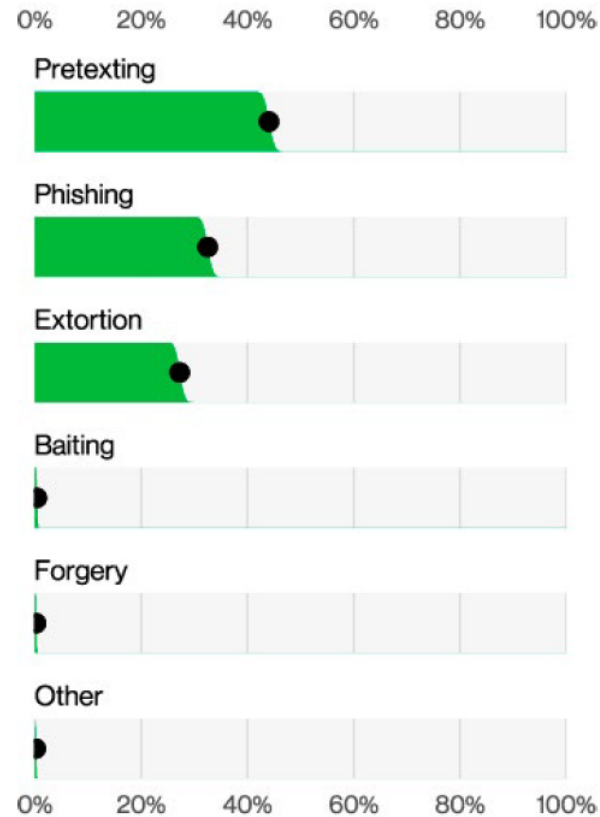


# Social Engineering & Pretexting

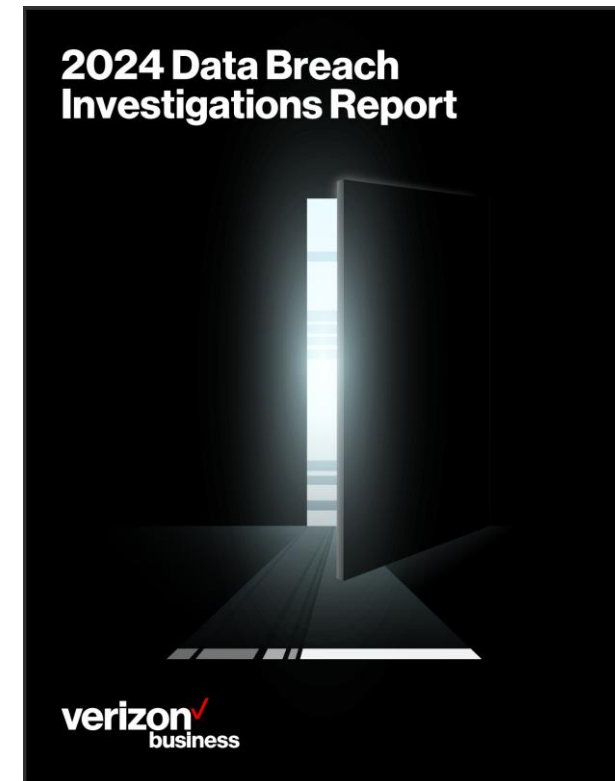
“Regardless of the exact method that attackers use to reach organizations, the core tactic is the same: They seek to exploit our human nature and our willingness to trust and be helpful for their own gain.”

While these attacks all share that commonality, one rather significant difference is the scale and pervasiveness of these tactics.”

Page 37



**Figure 34.** Top Action varieties in Social Engineering incidents (n=3,647)

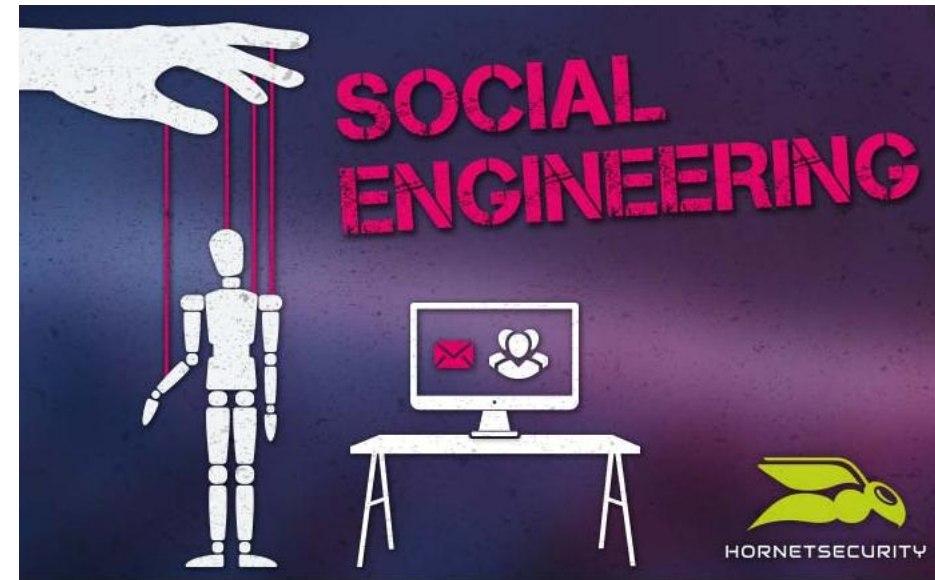






# Creating a Security Aware Organization

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



# 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

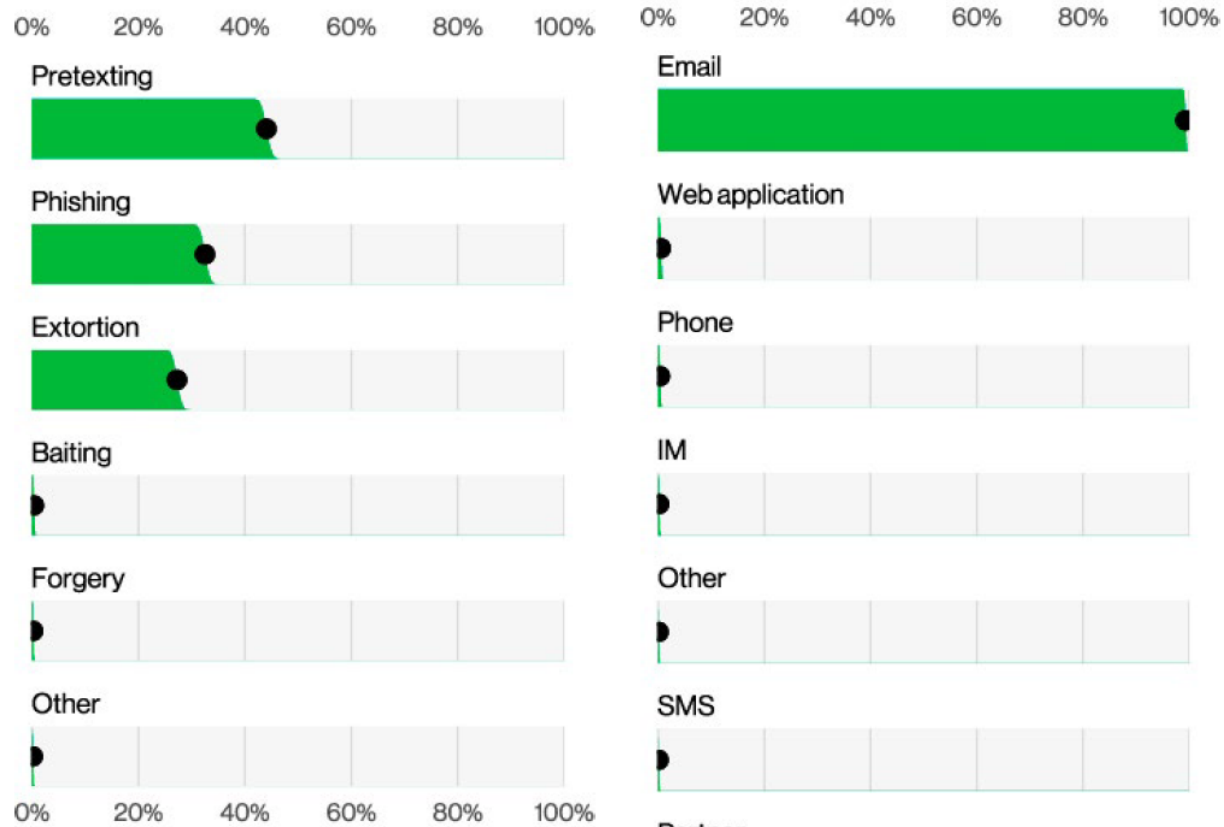


# Social Engineering

“Regardless of the exact method that attackers use to reach organizations, the core tactic is the same: They seek to exploit our human nature and our willingness to trust and be helpful for their own gain.

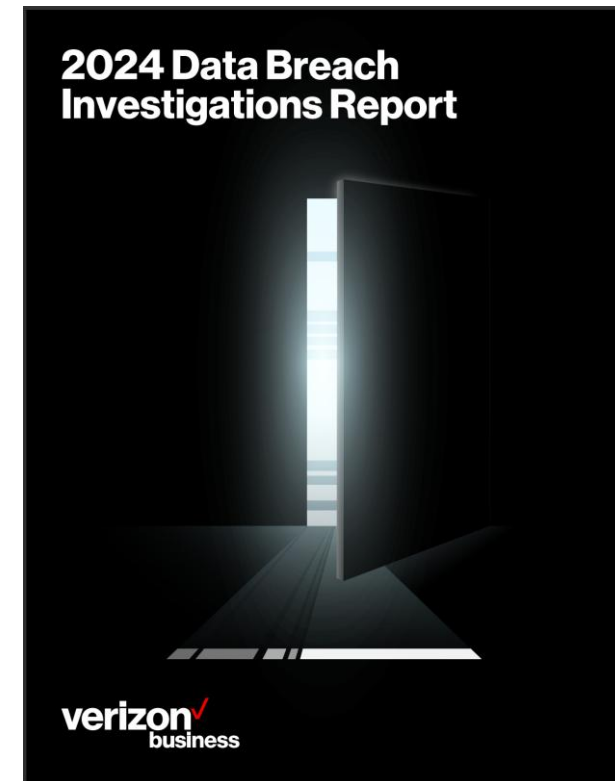
While these attacks all share that commonality, one rather significant difference is the scale and pervasiveness of these tactics.”

Page 37



**Figure 34.** Top Action varieties in Social Engineering incidents (n=3,647)

**Figure 35.** Top Action vectors in Social Engineering breaches (n=2,961)



# Phishing

“The first lesson to learn is that Phishing attacks happen fast.

The median time to click on a malicious link after the email is opened is 21 seconds, and then it takes only another 28 seconds to enter the data (Figure 39).

That leads to a frightening finding: The median time for users to fall for phishing emails is less than 60 seconds.”

Page 40

“Some good news is that, as an industry, we seem to be getting better with regard to phishing test reporting.

More than 20% of users identified and reported phishing per engagement, including 11% of the users who did click the email.”

Page 40

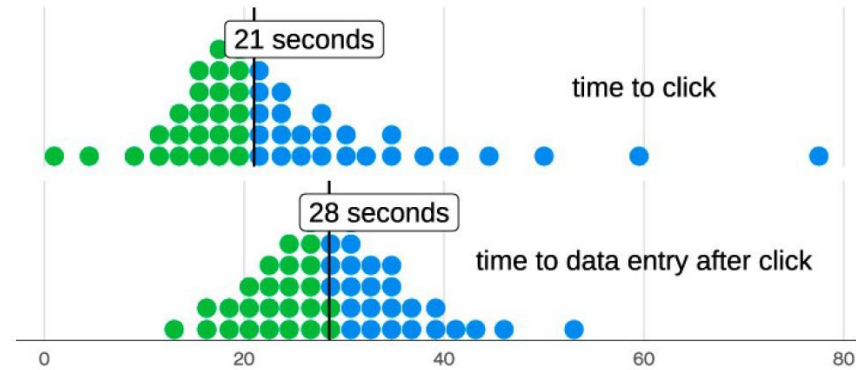


Figure 39. Time between email clicked and data entered

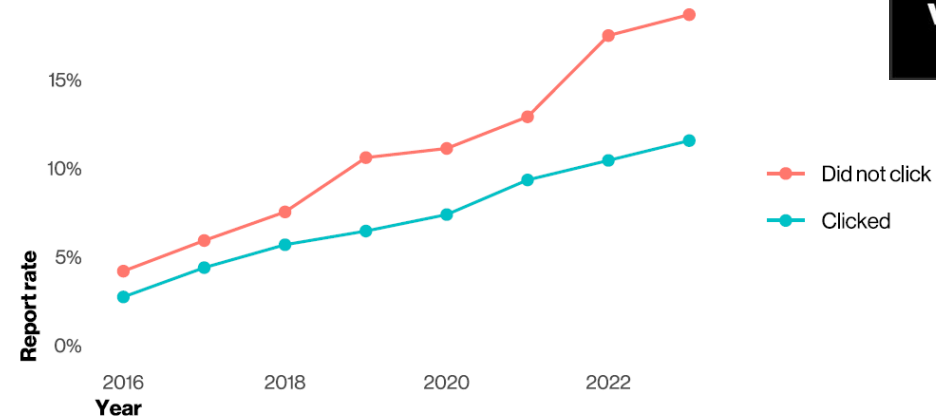
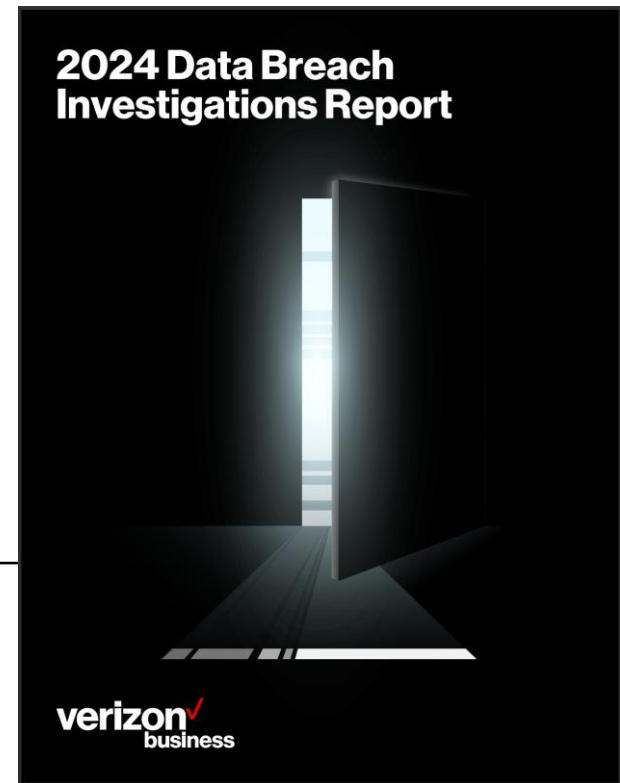


Figure 40. Phishing email report rate by click status



# “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  $\frac{1}{4}$  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

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

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

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

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

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

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

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

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

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

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

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 system

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 system

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

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

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

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

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

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# 2b -

## Creating a Security Aware Organization