

# Managing Enterprise Cybersecurity

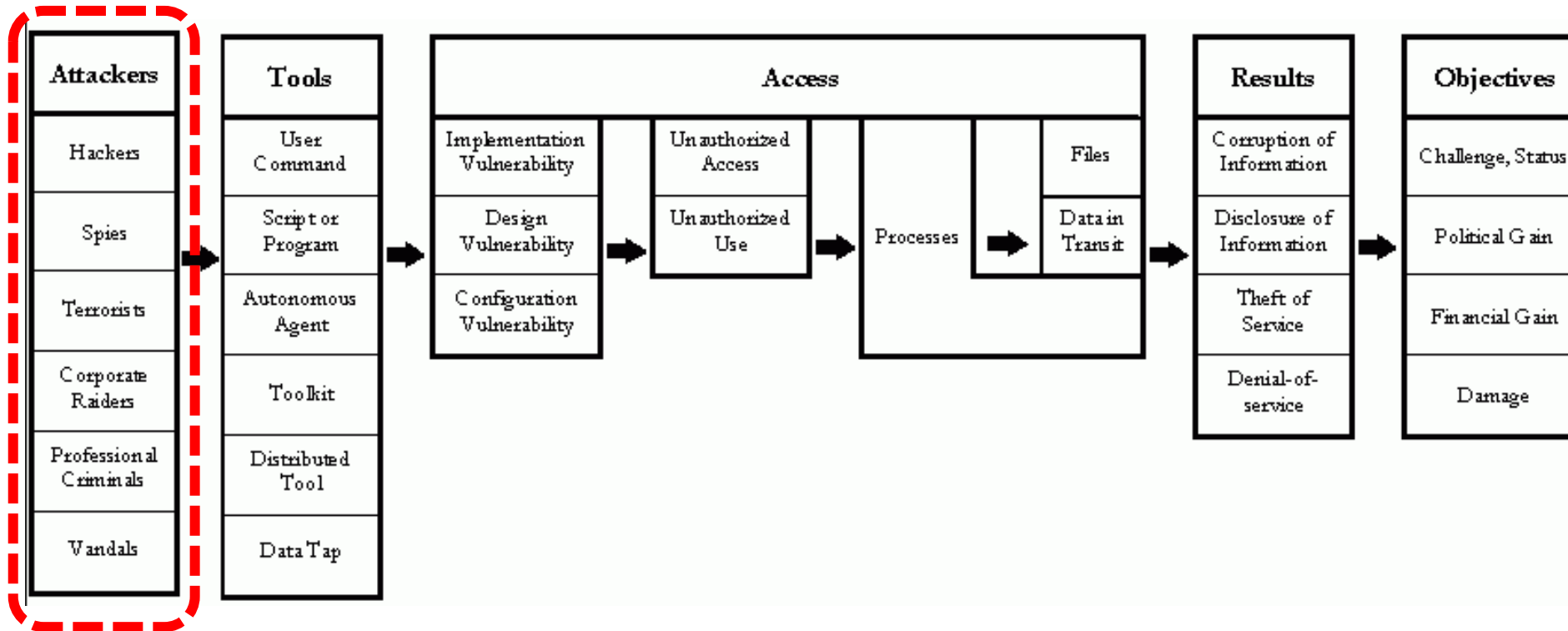
## MIS 4596

Human Element of Security

Unit #16

# 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.*

# Agenda

- Human element of cyber security
- Employee risk
- Cyber security employee awareness and training risk controls
- Insider threat
- Social Engineering
- Some thoughts about cyber security training programs

# Vulnerabilities

Inadequacies in any of these areas:

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


NIST Special Publication 800-53  
Revision 5

## 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>

September 2020  
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII



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*

## 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

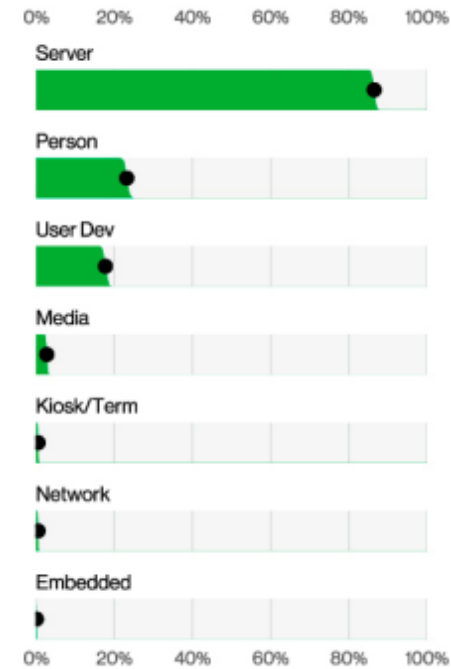
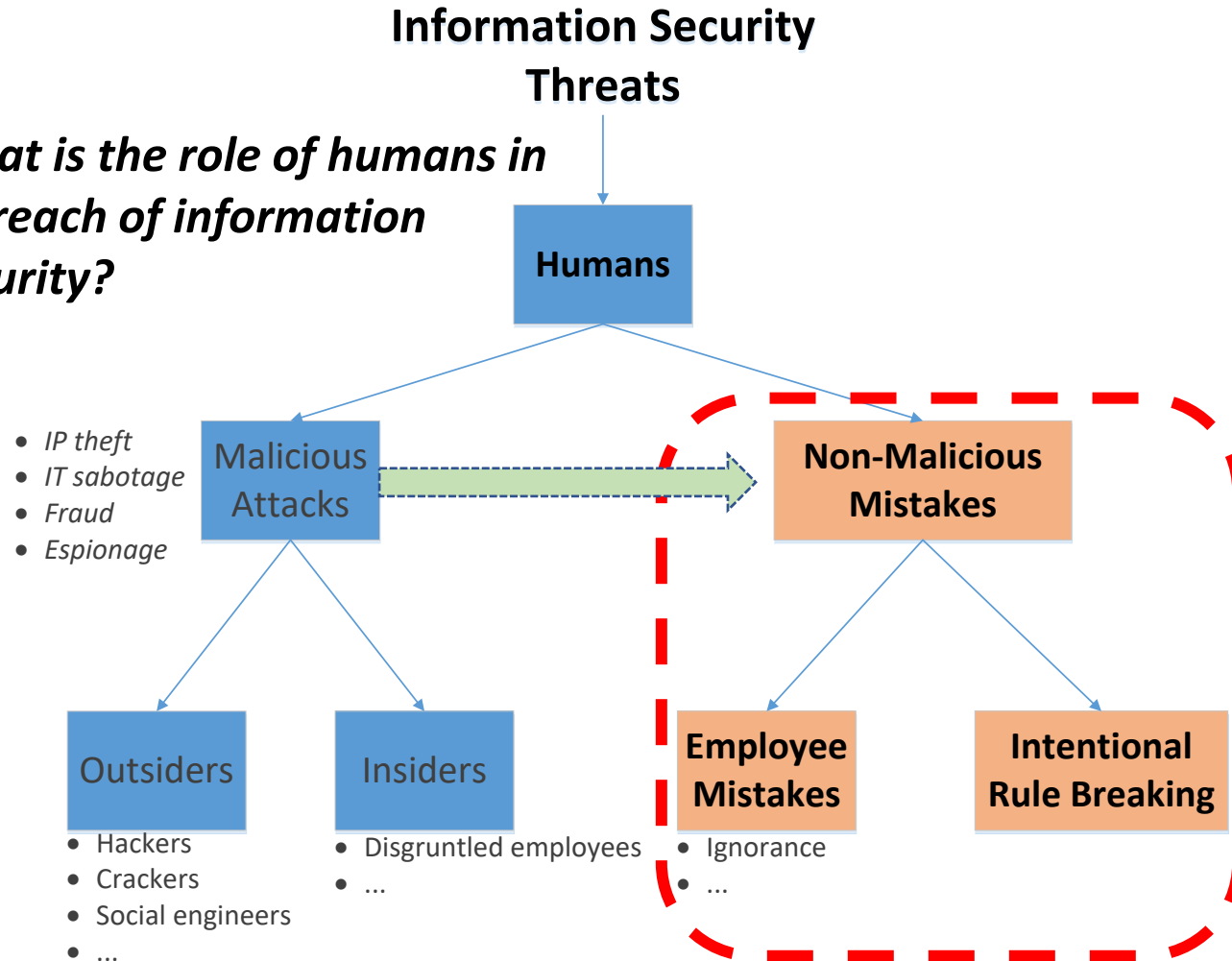
National Institute of Standards and Technology  
 Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

TABLE 3-2: AWARENESS AND TRAINING FAMILY

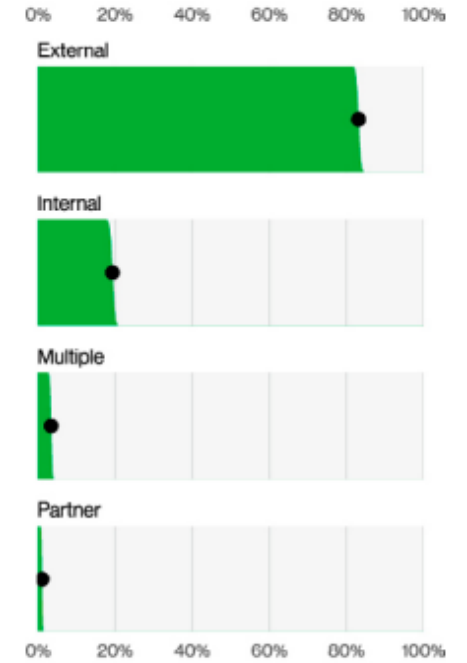
CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	Policy and Procedures	X	X	X	X
AT-2	Literacy Training and Awareness	X	X	X	X
AT-2(2)	INSIDER THREAT		X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			X	X
AT-3	Role-Based Training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

# The threat landscape....

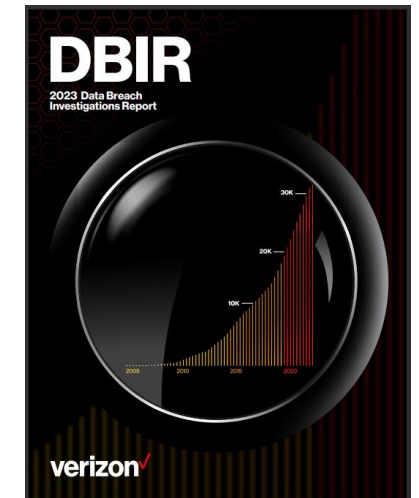
*What is the role of humans in a breach of information security?*



**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

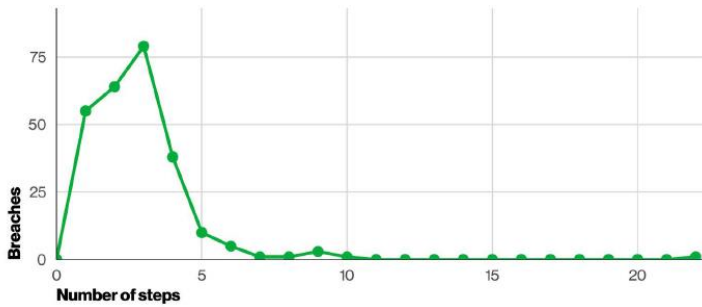
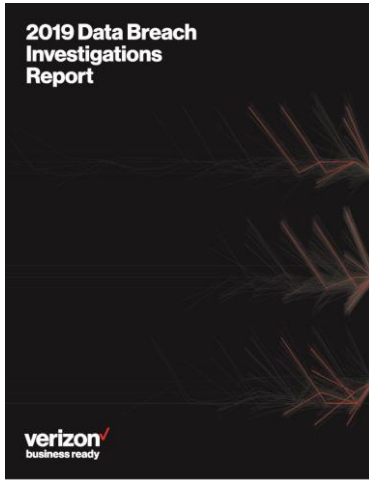


Figure 30. Number of steps per breach in non-Error breaches (n=258)

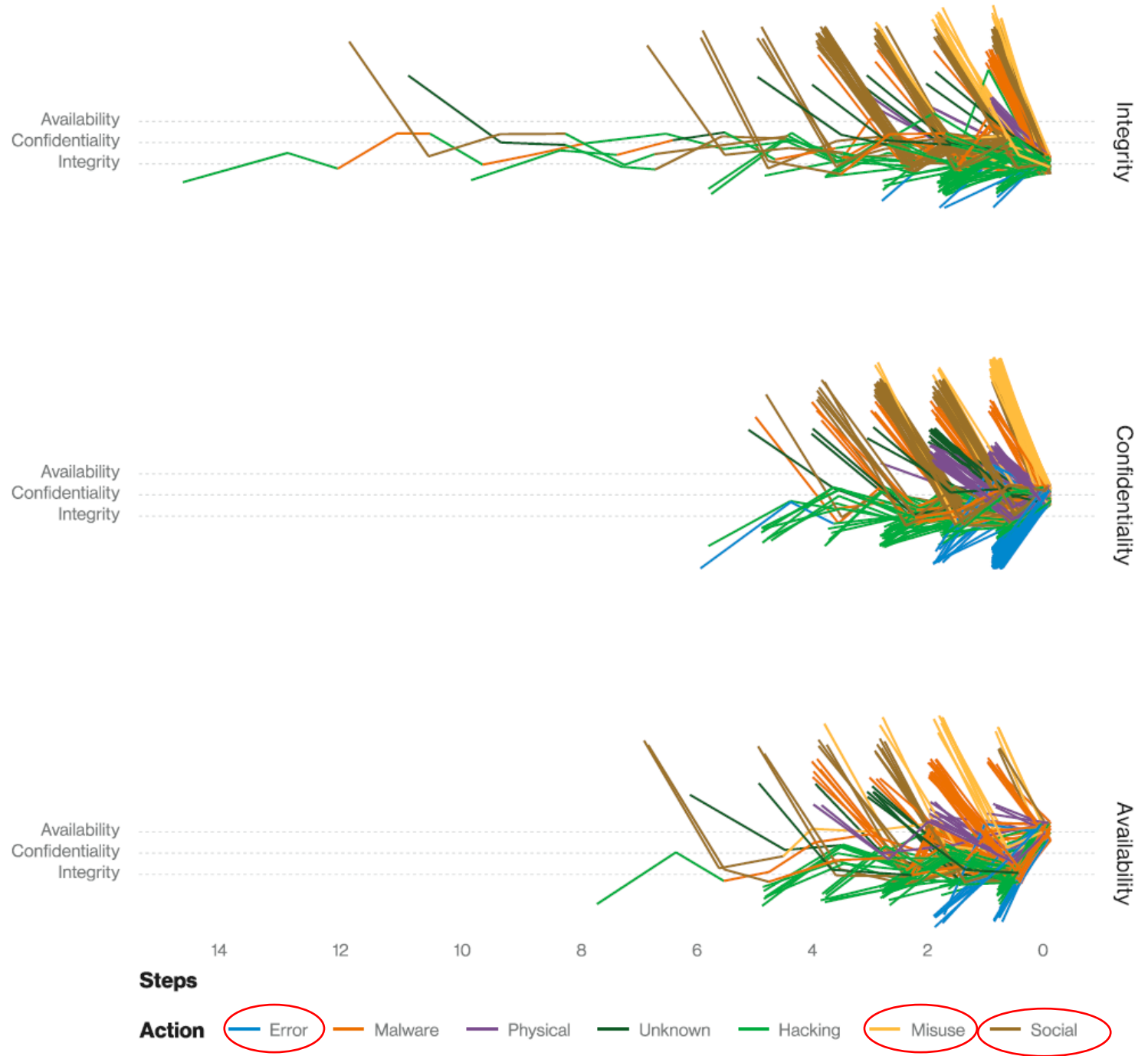


Figure 30. Attack chain by final attribute compromised<sup>12</sup> (n=941)

Figure 1: ENISA Threat Landscape 2022 - Prime threats

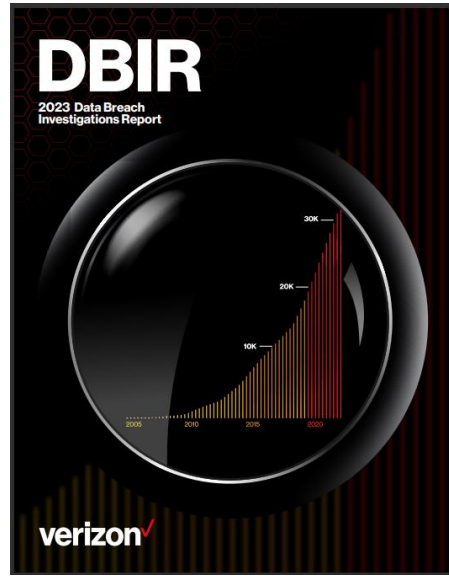
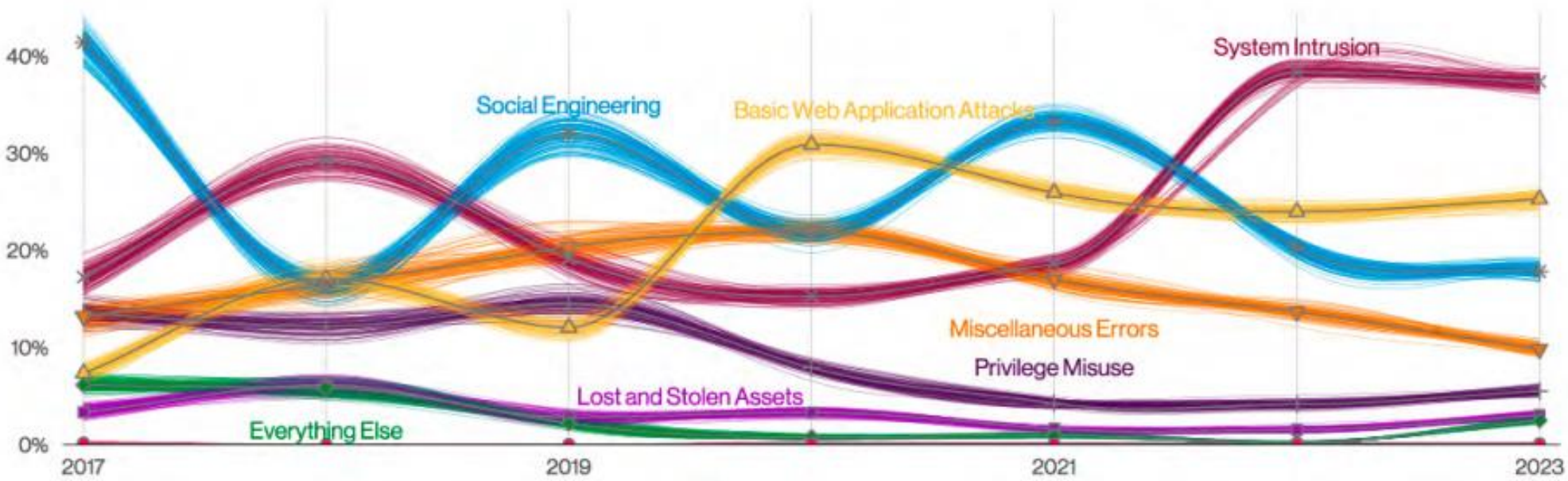


***In which of these threats are humans the vulnerability?***





# 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 areas...

# Employee Risk

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

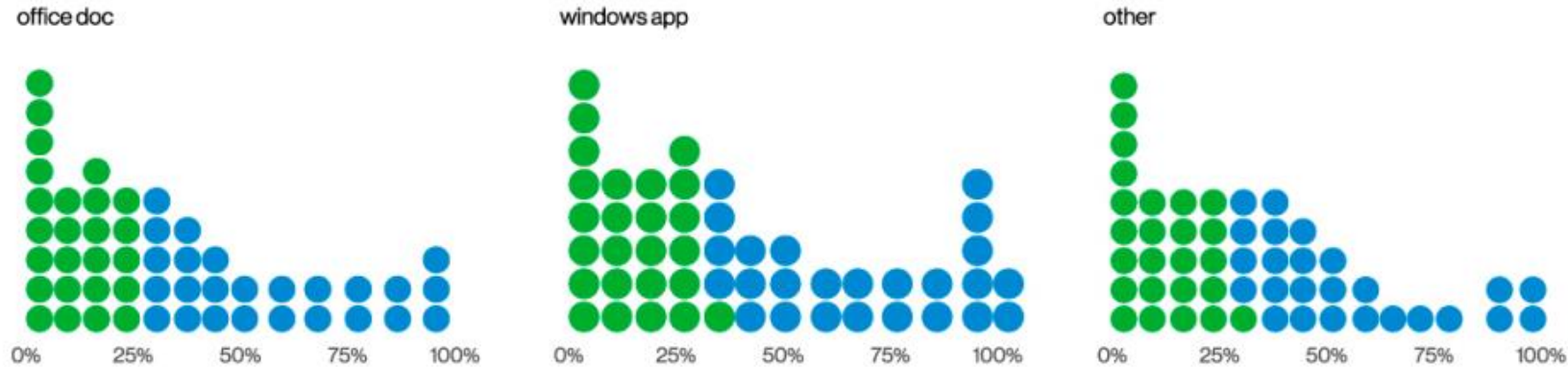
- Organizations must also ensure their security posture is good by:
  - Setting policies, educating staff, and enforcing good security hygiene
  - Taking advantage of the security options that are available
  - Training and testing employees
  - Implementing automated checks to ensure their security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

# Employee Risk

## Malware delivery methods

*“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)

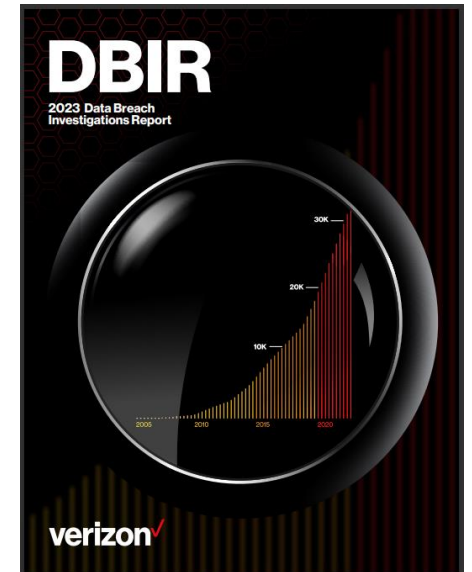
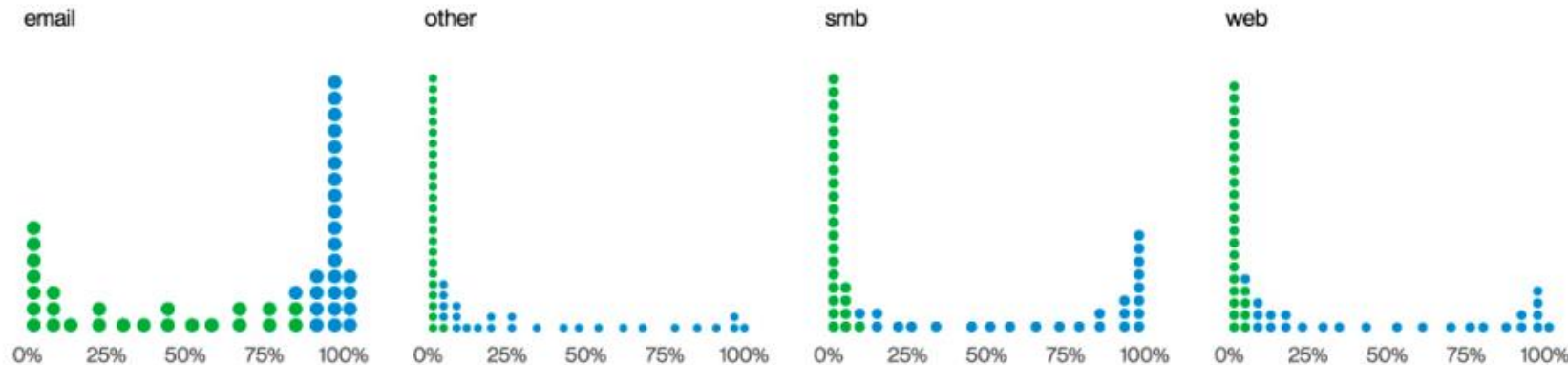
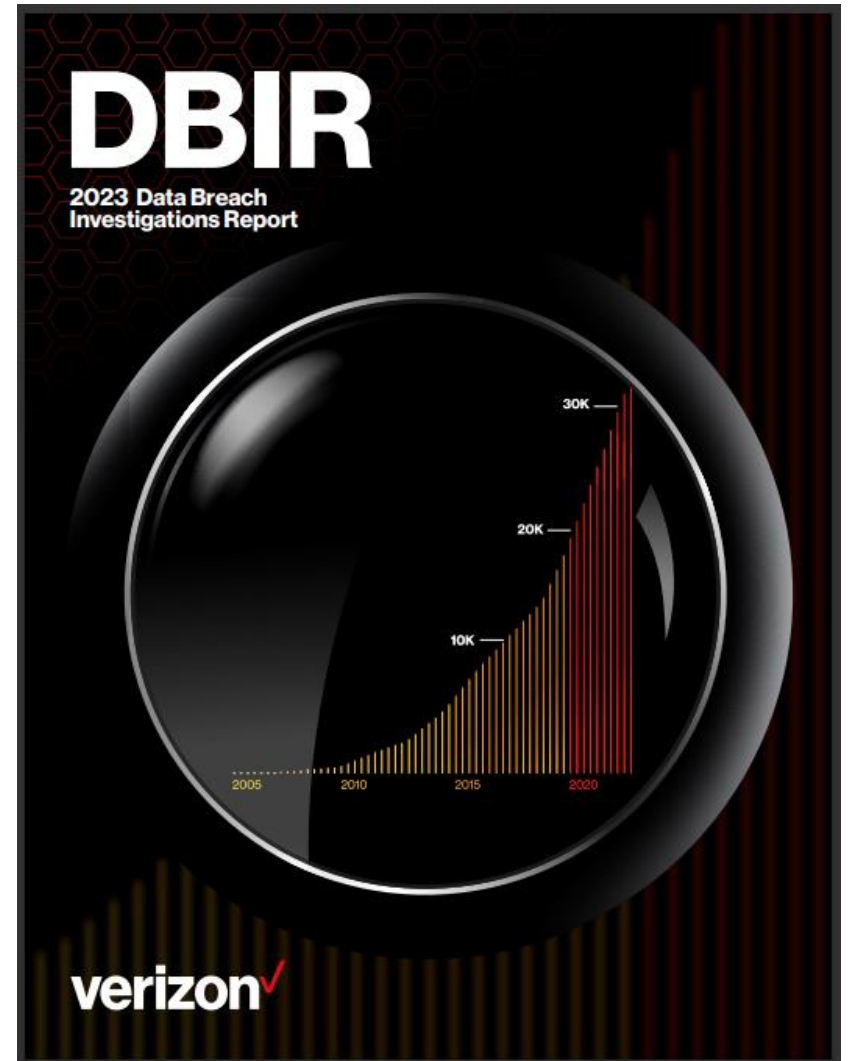


Figure 30. Malware delivery method proportion per organization



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



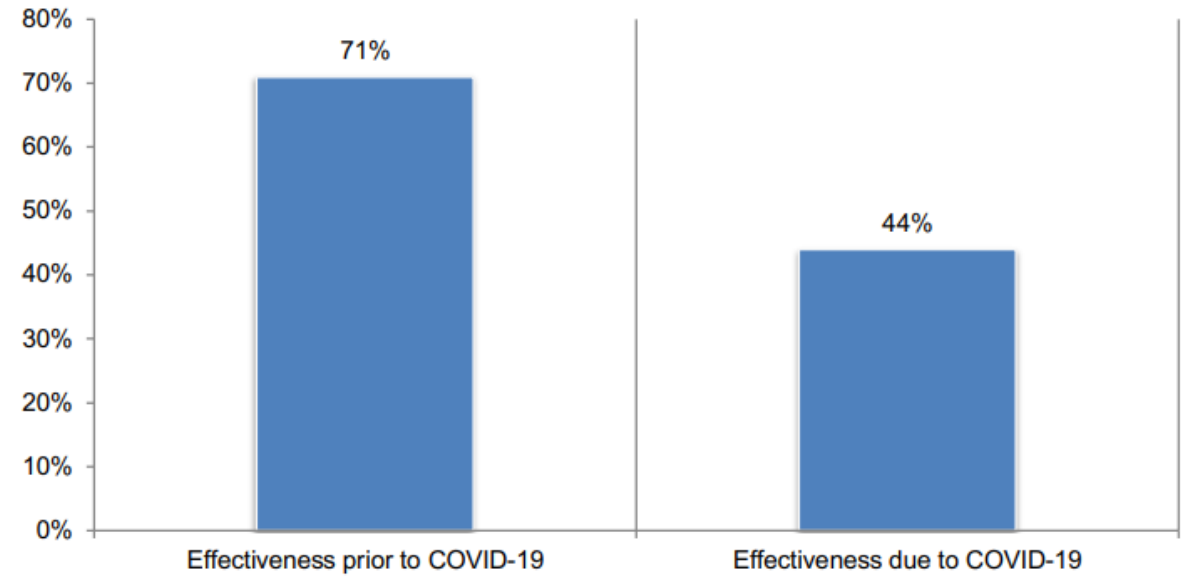
# Cybersecurity in the Remote Work Era:

## 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

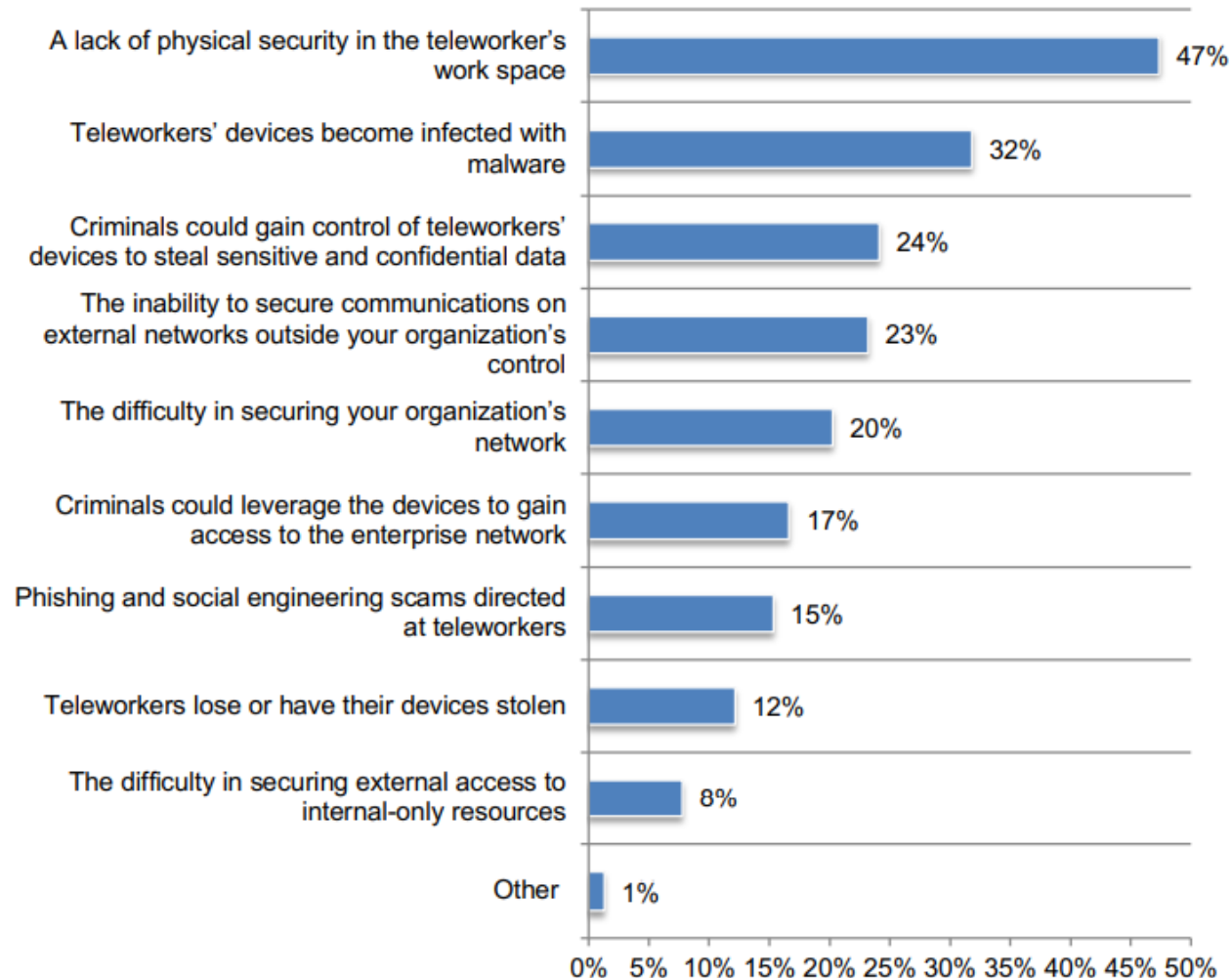
Sponsored by Keeper Security, Inc.  
Independently conducted by Ponemon Institute LLC



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:

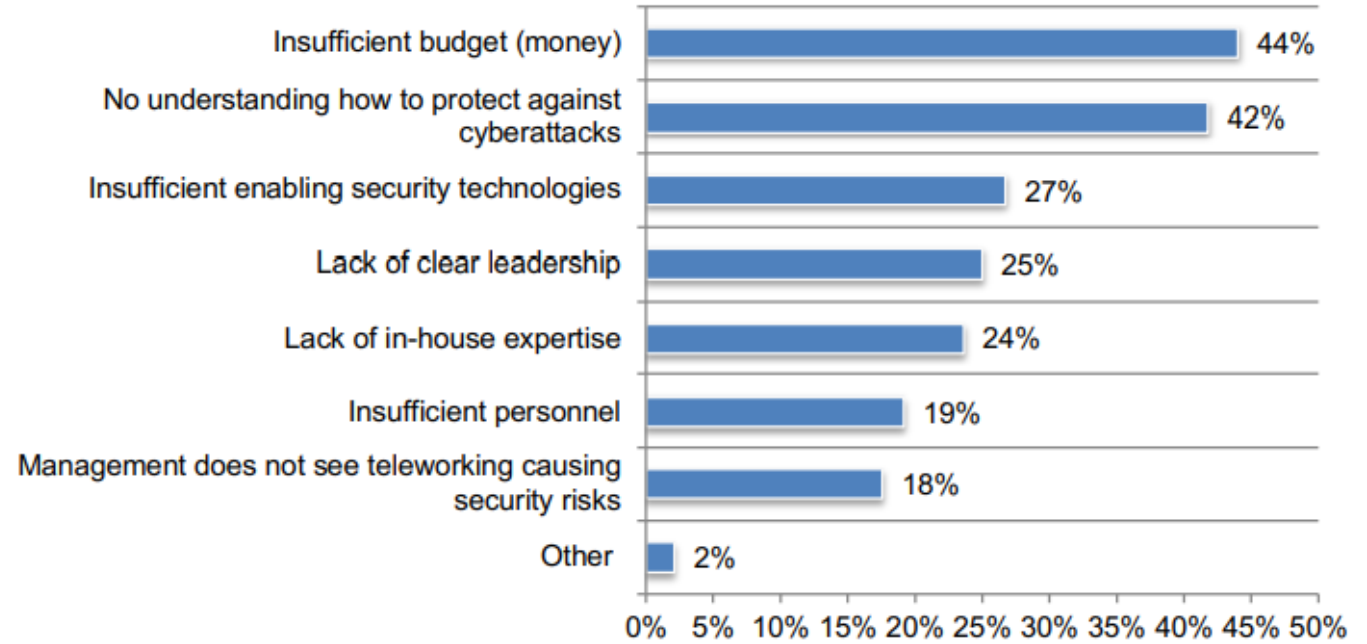
A Global Risk Report

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



## 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

TABLE 3-2: AWARENESS AND TRAINING FAMILY

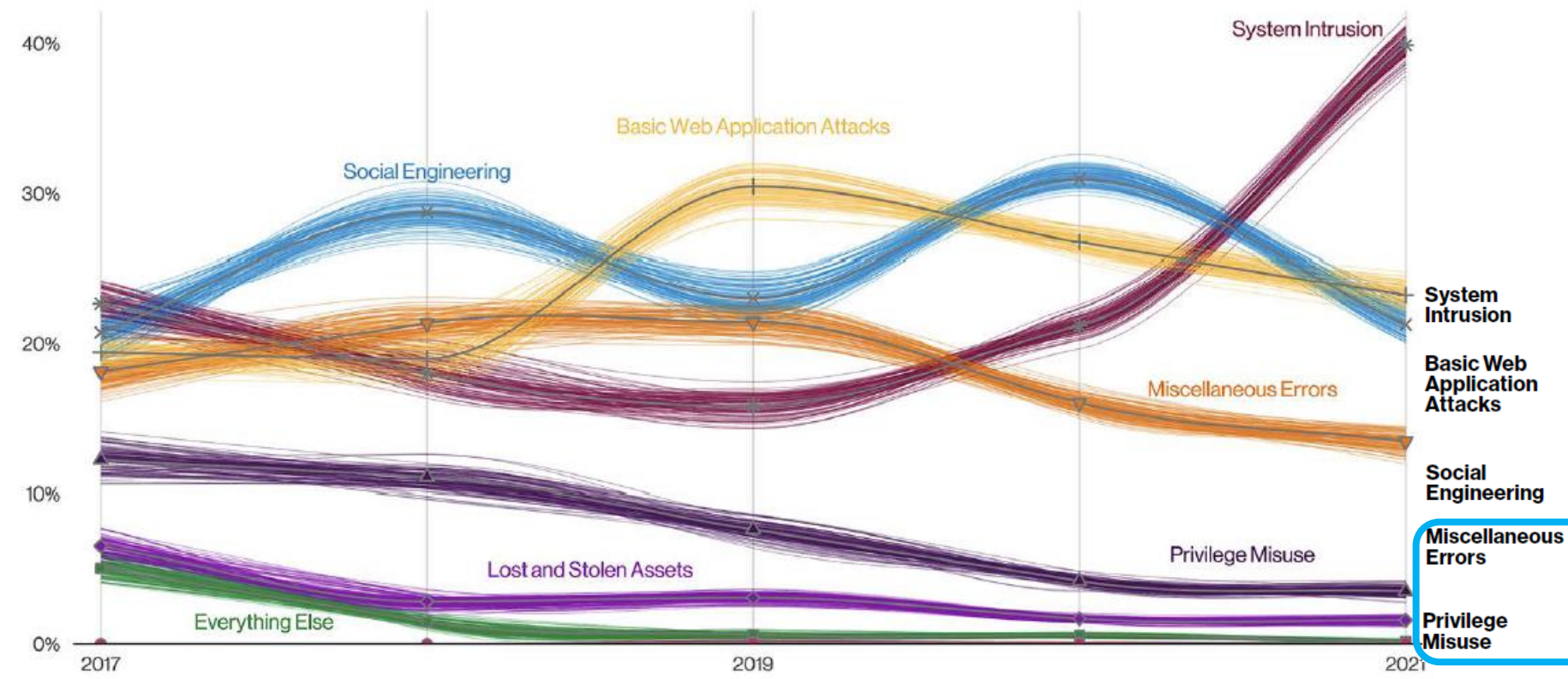
CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	Policy and Procedures	X	X	X	X
AT-2	Literacy Training and Awareness	X	X	X	X
AT-2(2)	INSIDER THREAT		X	X	X
AT-2(3)	SOCIAL ENGINEERING AND MINING			X	X
AT-3	Role-Based Training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







# Patterns in breaches – Insider Threat



**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.

Figure 33. Patterns over time in breaches

# 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...

## 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...”

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

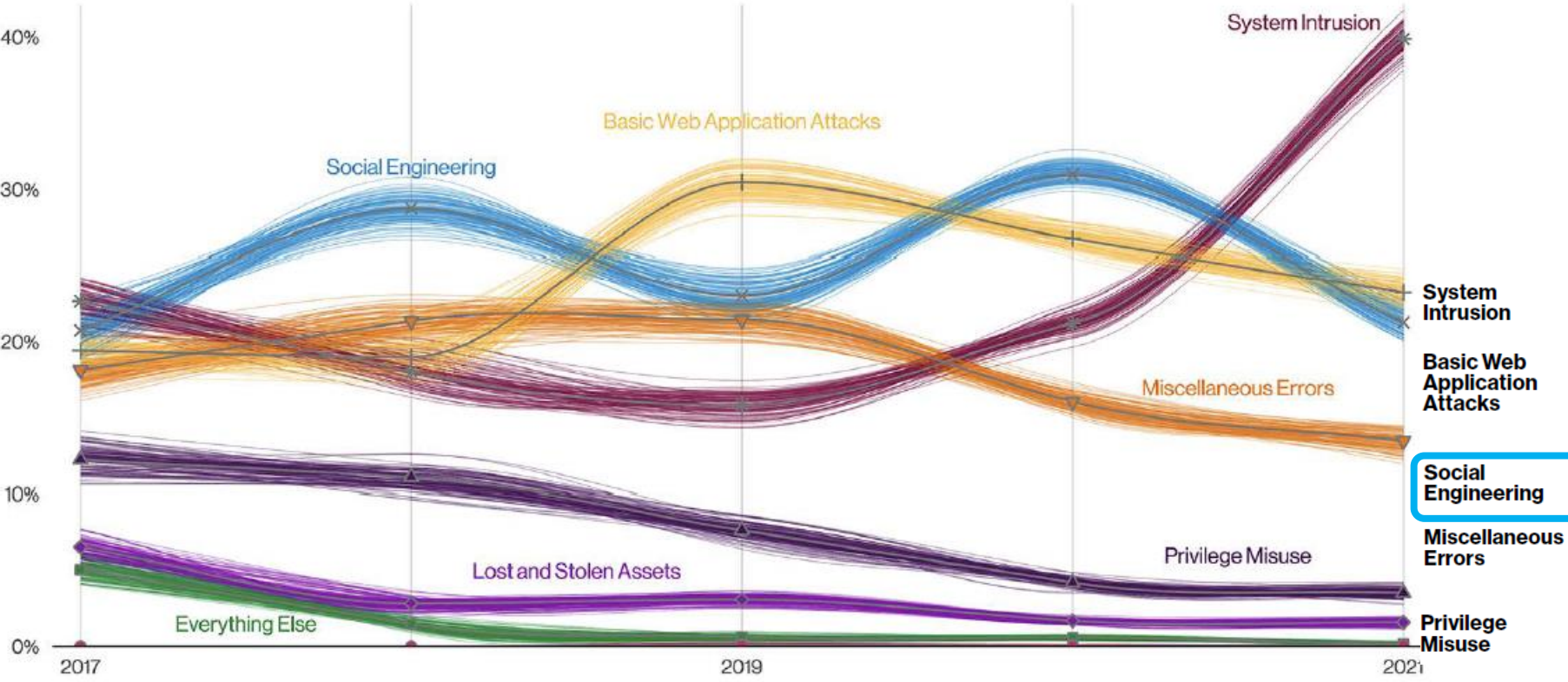


U.S. Department of Commerce  
 Wilbur L. Ross, Jr., Secretary

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



# Patterns in breaches



Complex attacks that leverage malware and/or hacking to achieve their objectives including deploying Ransomware.

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.

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.

Incidents predominantly driven by unapproved or malicious use of legitimate privileges.

Figure 33. Patterns over time in breaches

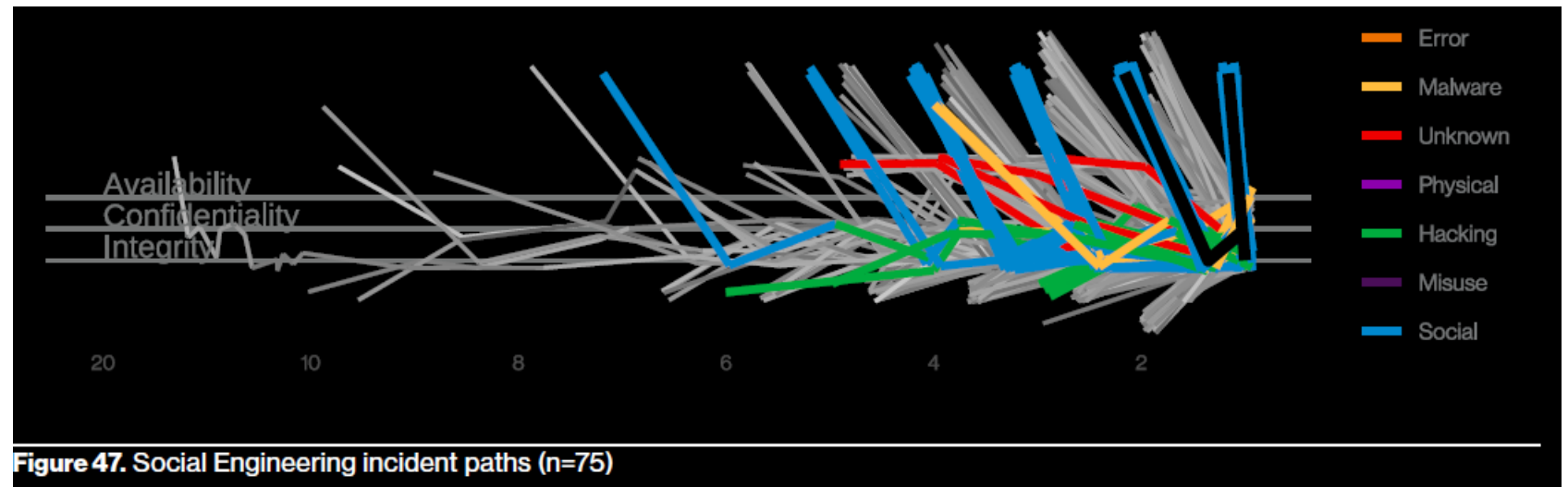


# Social Engineering

- 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*



# 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

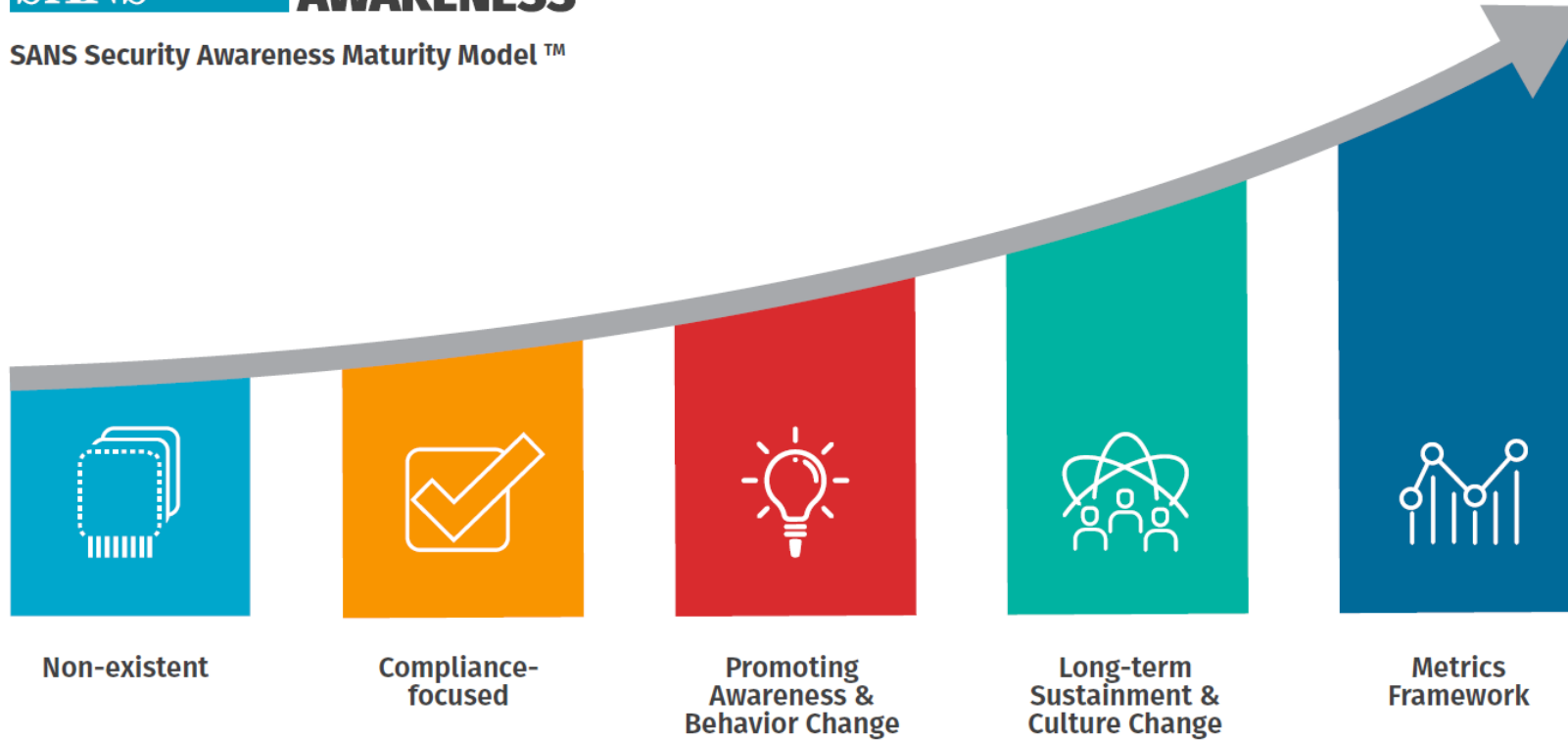
- Refusal to give call back number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of non-compliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting



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



SANS Security Awareness Maturity Model™



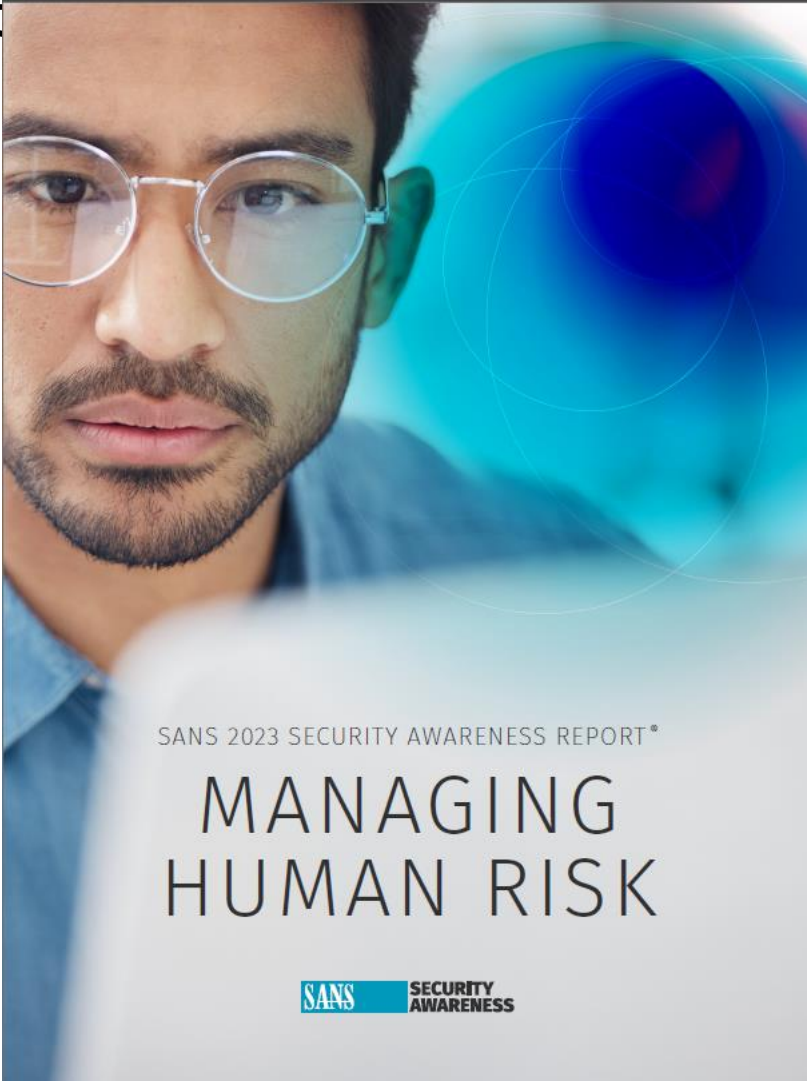
Non-existent

Compliance-focused

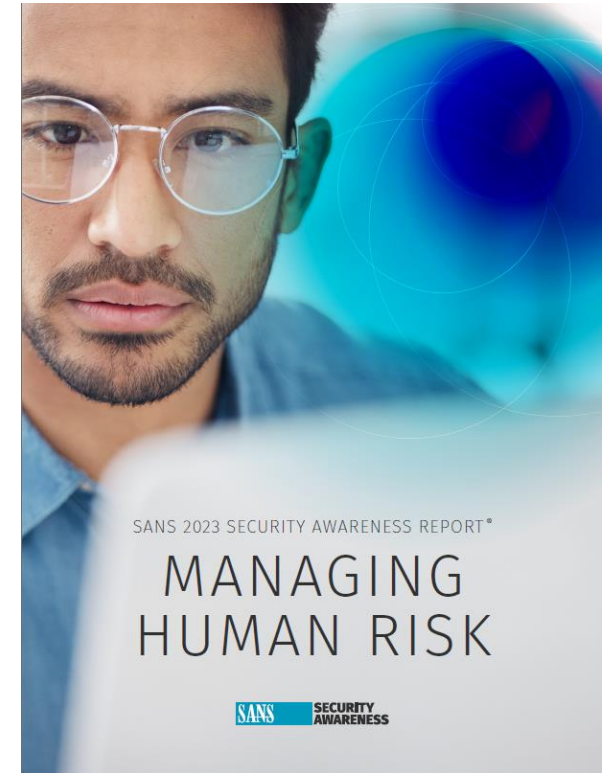
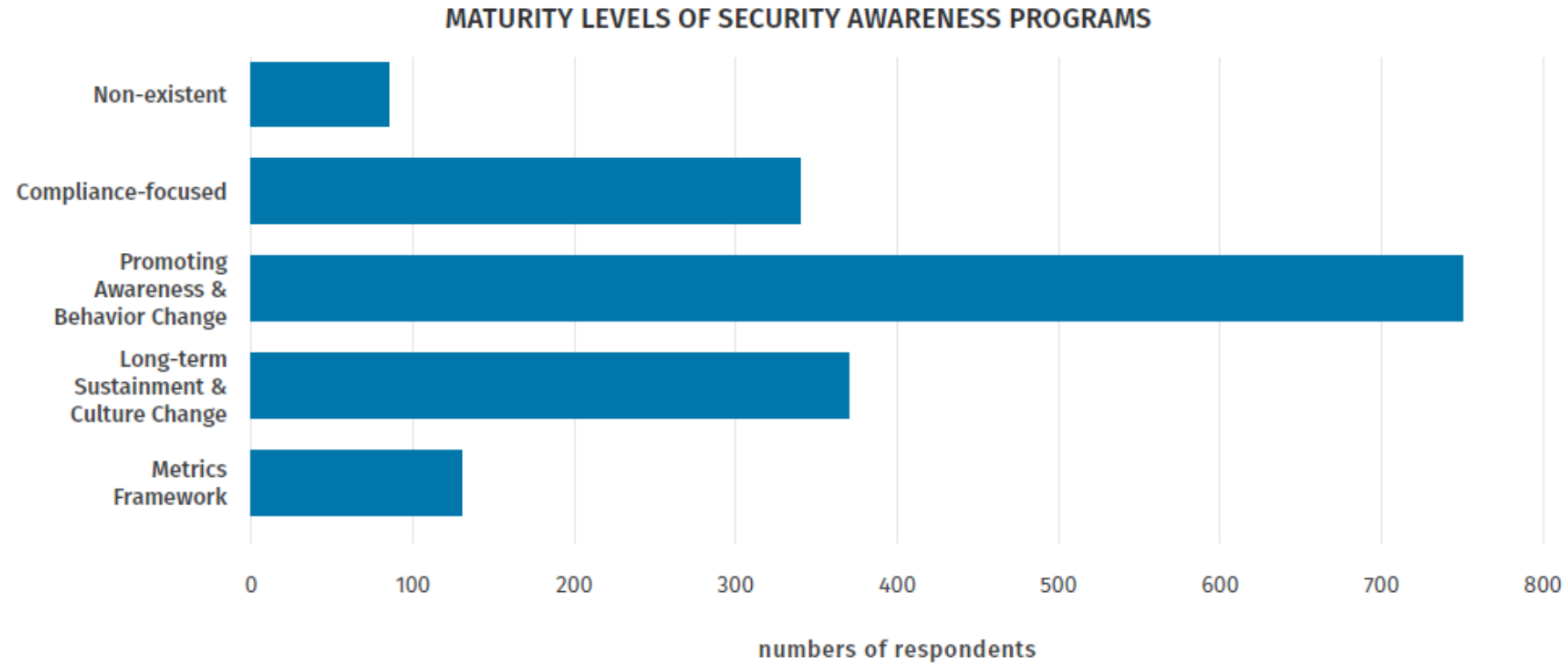
Promoting Awareness & Behavior Change

Long-term Sustainment & Culture Change

Metrics Framework

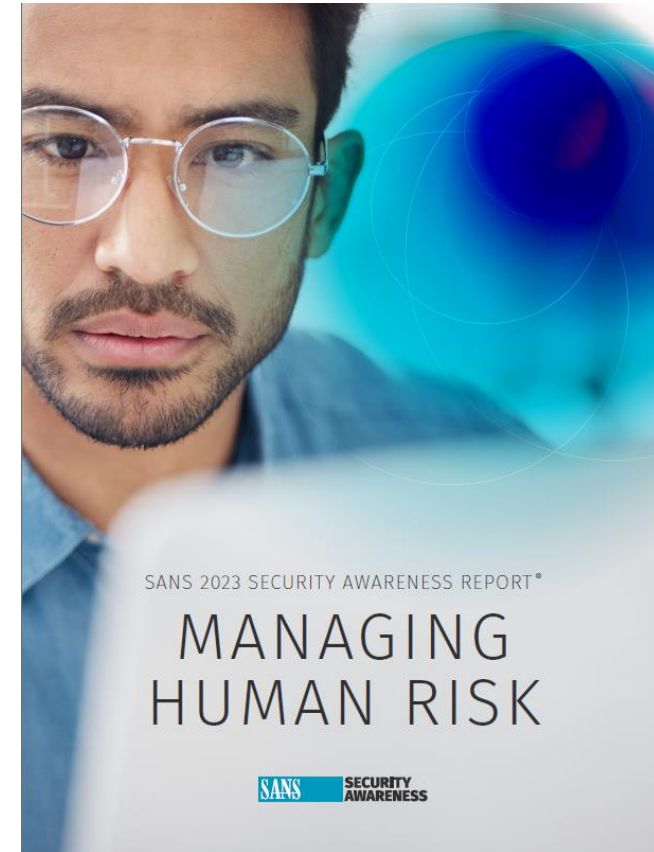
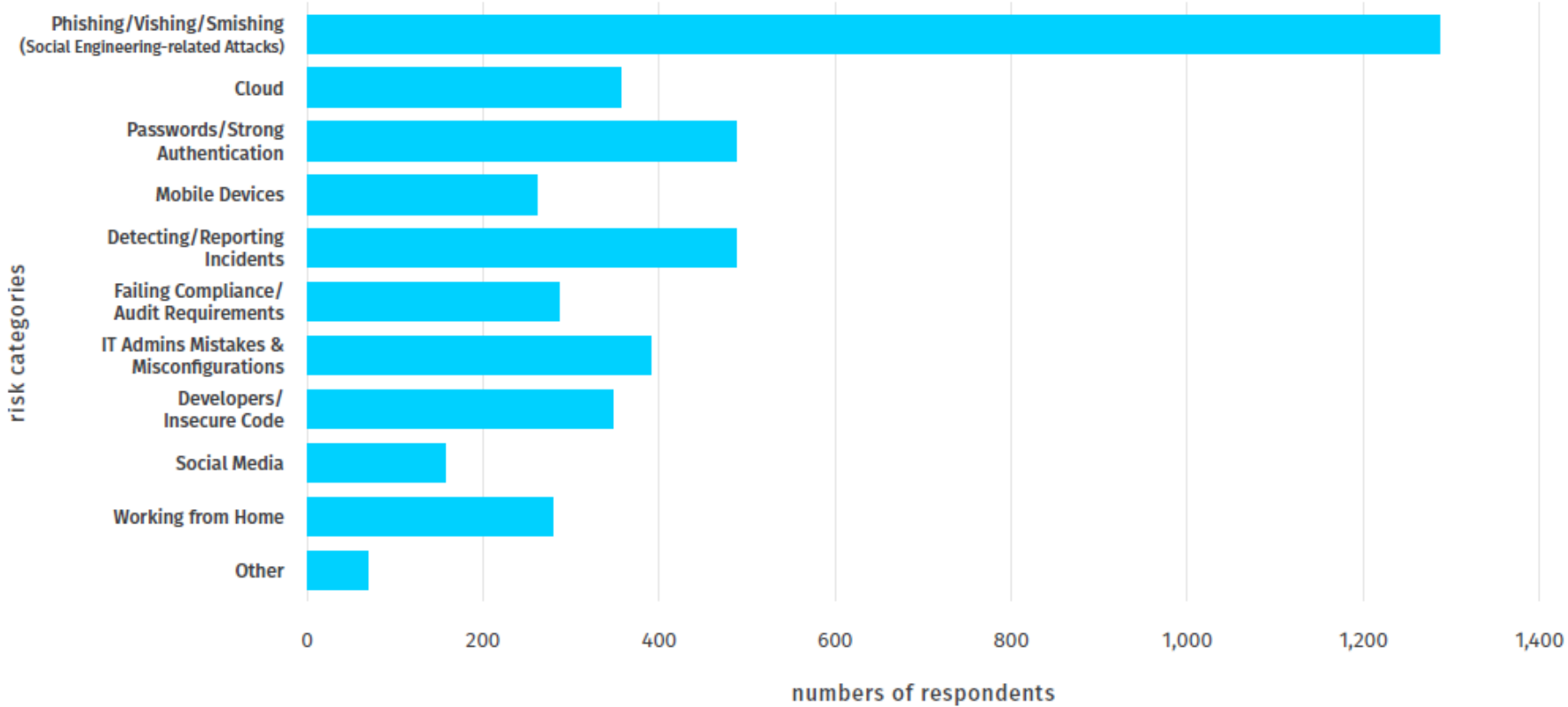


<https://www.sans.org/blog/sans-2022-security-awareness-report/>

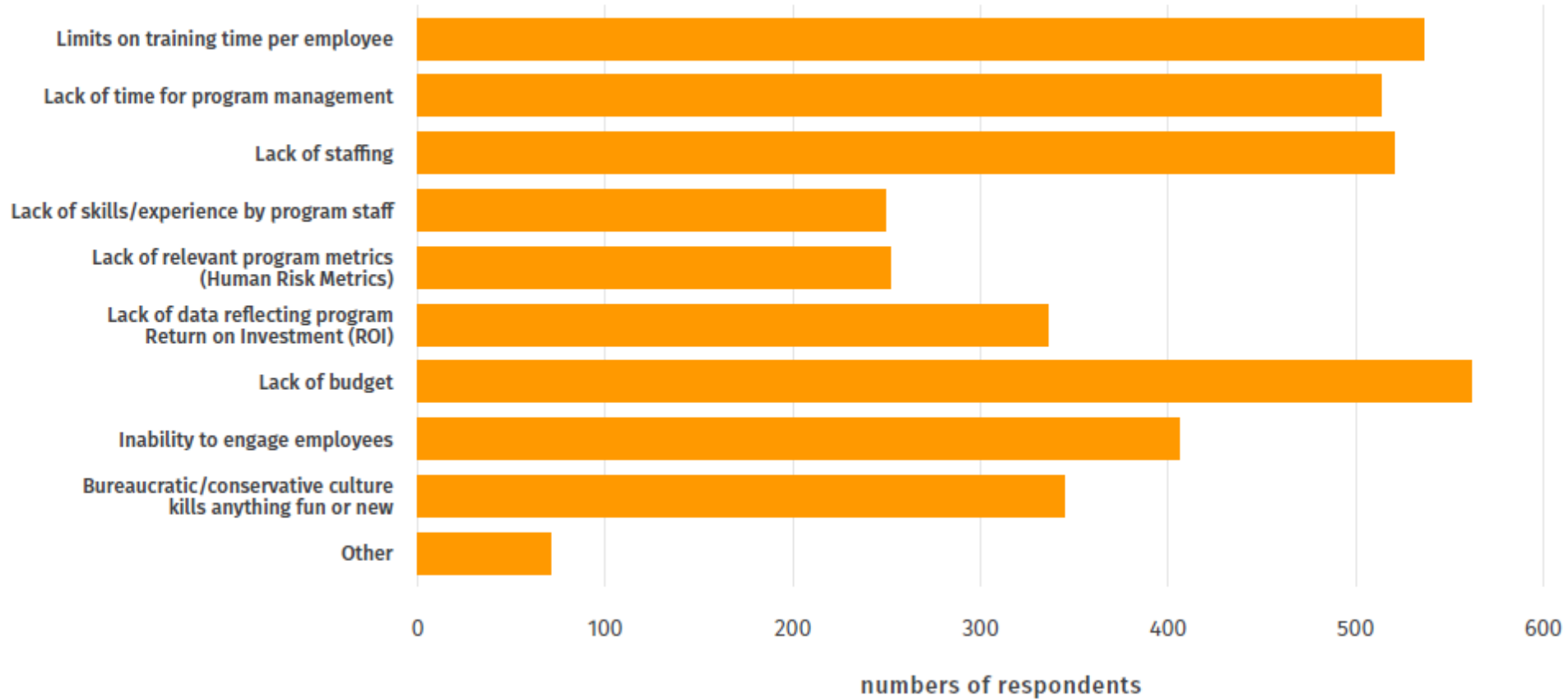


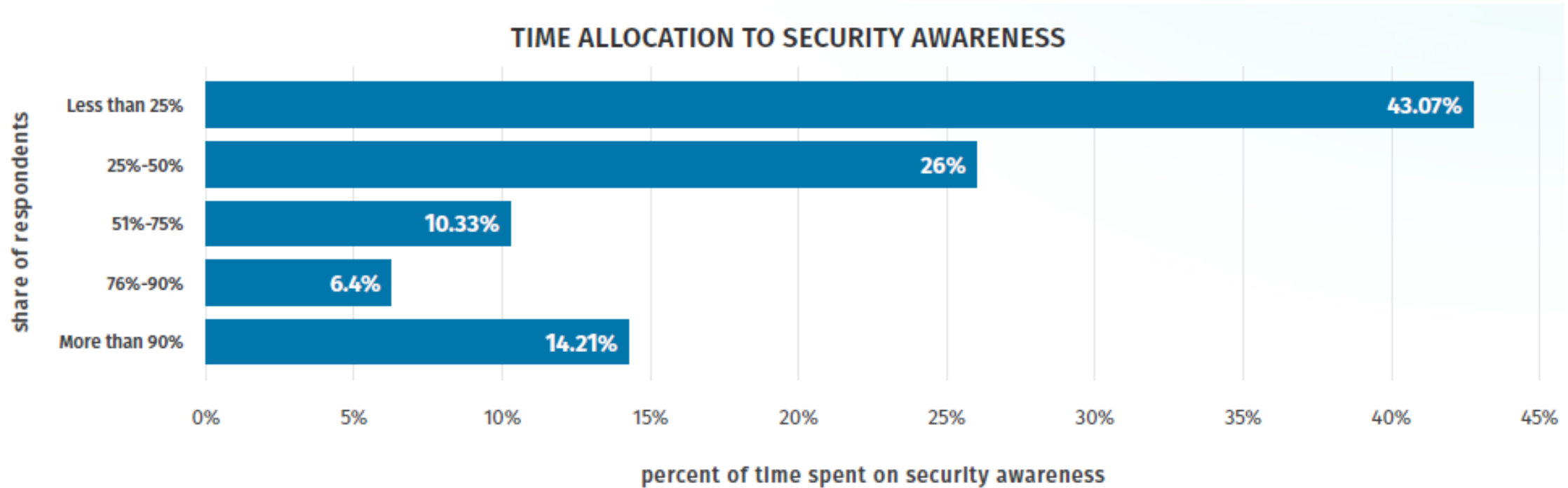


### TOP HUMAN RISKS TO ORGANIZATIONS



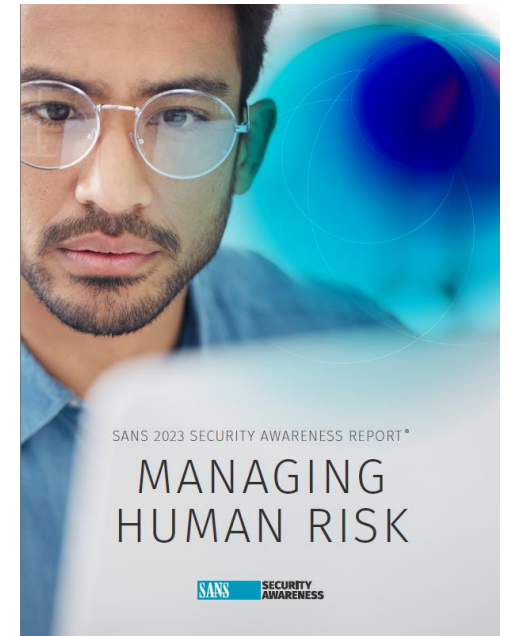
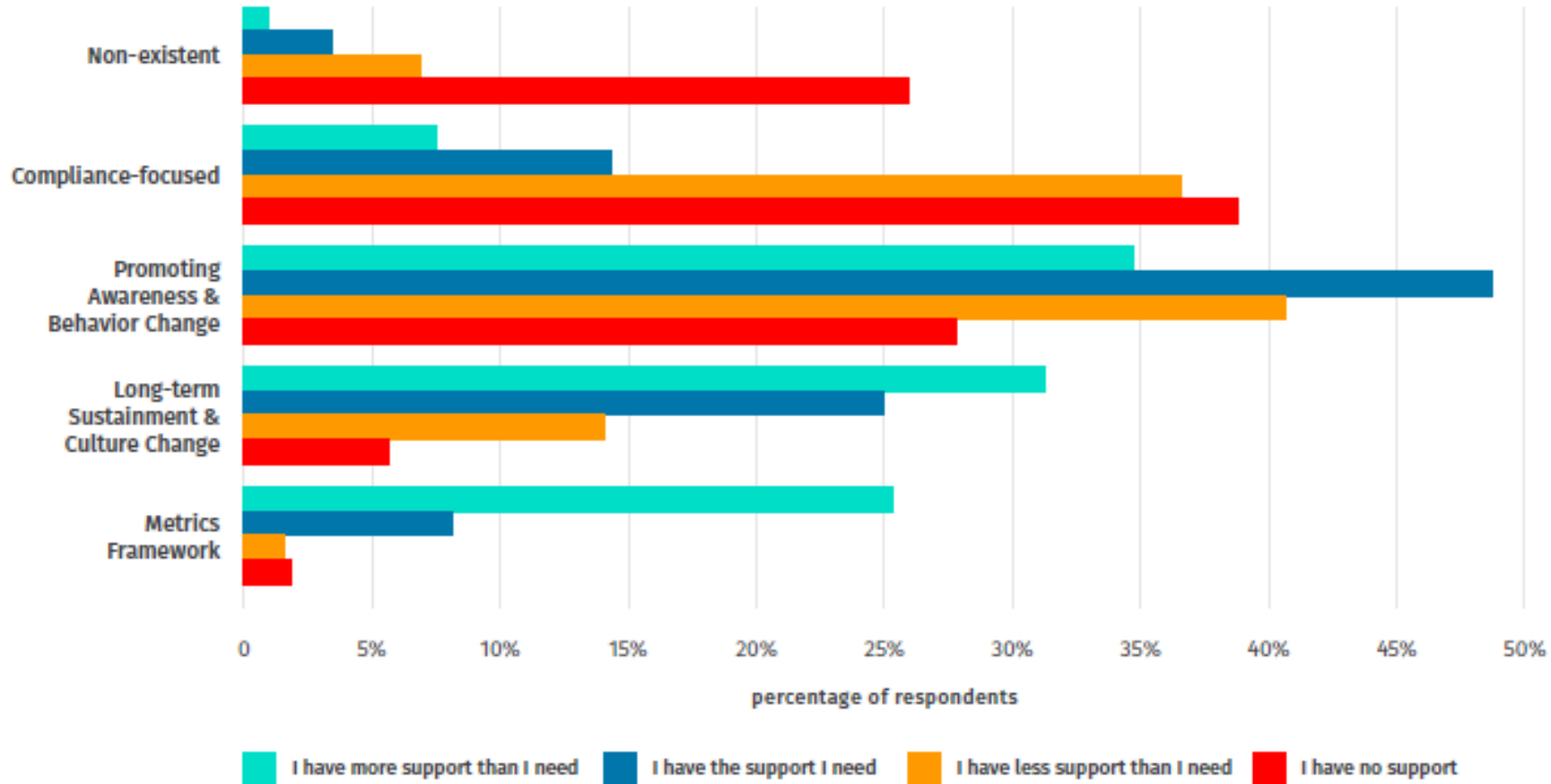
### PROGRAM CHALLENGES





“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**



# Agenda

- ✓ Human element of cyber security
- ✓ Employee risk
- ✓ Cyber security employee awareness and training risk controls
- ✓ Insider threat
- ✓ Social Engineering
- ✓ Some thoughts about cyber security training programs