Protecting Information Assets
- Unit# 5 -

Creating a Security
Aware Organization

Agenda

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

Updated [Schedule](#) in [Syllabus](#)

MIS5206 Section 701   **Syllabus**   **Page** 3

Schedule:

Unit	Assignment Topics	Date
1	Introduction to MIS5206	Aug. 25
1	Understanding an Organization's Risk Environment	Aug. 25
2	Case Study 1: *Snowfall and a stolen laptop*	Sept. 1
2	Data Classification Process and Models	Sept. 1
3	Risk Evaluation	Sept. 8
	Class will not be held on September 15th	*Sept. 15*
4	Case Study 2: *Autopsy of a Data Breach: The Target Case*	Sept. 22
5	Creating a Security Aware Organization	Sept. 29
6	Physical and Environmental Security	Oct. 6
7	**Midterm Exam**	Oct. 8-10
8	Case Study 3: *A Hospital Catches the "Millennium Bug"*	Oct. 13
9	Business Continuity and Disaster Recovery Planning	Oct. 20
10	Network Security	Oct. 27
11	Cryptography, Public Key Encryption and Digital Signatures	Nov. 3
12	Identity Management and Access Control	Nov.10
13	Computer Application Security	Nov. 17
13	Team Project Presentations	Nov. 17
14	Review	Dec.1
14	Team Project Presentations	Dec.1
15	**Final Exam**	Dec. 15

MIS 5206 Protecting Information Assets

In The News

Christopher Clayton says

SEPTEMBER 24, 2021 AT 2:00 PM

(Edit)

"85% of UK's Top Universities at Risk of Email Fraud"

Proofpoint, an enterprise security company based in California, did a study on universities in the UK, and shown that out of the top 20 colleges, 85% were at risk of email fraud, and only a small percentage have applied a domain-based message authentication (DMARC), an email validator that confirms who the sender is. Schools and colleges have been a key target for cybercriminals to trick students through spear-phishing attacks ever since the pandemic. Within the last couple of years, the majority of those top colleges have identified the need to apply DMARC procedures for their institutions, however, only a few have yet to do so. The cybersecurity strategist at Proofpoint mentioned that UK universities are still not taking proper measures to prevent cybercriminals from getting access to their data, and that authentication procedures such as using DMARC is a crucial instrument in email fraud defenses.

https://www.infosecurity-magazine.com/news/uk-universities-risk-email-fraud/

https://dmarc.org/overview/

In The News

Bryan Garrahan says
SEPTEMBER 28, 2021 AT 10:47 PM

(Edit)
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/improving-cybersecurity-awareness-through-hacking

This blog from ISACA attempts to explore ways in which organizations should facilitate their security awareness and training programs. The article notes that many organizations tend to utilize and require their employees to partake in the same Cybersecurity trainings year over year. Kris Martel, who wrote the blog, notes that these trainings are essentially ineffective as hackers are aware of the principles taught in the trainings and he believes they do not prepare an organizations employees to protect themselves. Furthermore, Martel notes that hackers are constantly evolving their skills to identify new attack vectors, which are not always included or updated within an organizations Cybersecurity awareness and training program. Martel writes, "Cybercriminals are always looking for new ways to infiltrate and attack organizations. So why not think like the enemy and create a cybersecurity awareness training program that resembles what the real cybercriminals will do?" Martel believes it's essential for an organization to make the training feel personnel and interactive so that employees can actually decipher how a security incident could effect them. Martel finishes the blog stating, "Branding your cyber awareness training as a monthly opportunity to hack your coworker and then showing them how the cyber criminals are "hacking" the user will increase awareness and strengthen cybersecurity practices".

[In The News](#)

Miray Bolukbasi says

SEPTEMBER 28, 2021 AT 11:37 PM

(Edit)

Since our lecture topic will be security awareness and training this week, I picked a relevant article that would address some of the real life issues in lack of SETA. The article simply talks about the increase in the cyberattacks since the organizations in UK have transformed their business operations to online during covid-19 outbreak. The president of the EU commission warns employers about attackers that are attracted by remotely working employees.

Recent research by Promon explains that two-thirds of remote employees are not given training in the past 12 months for security awareness and 77% of them not feeling worried about cyberattacks can happen due the new working conditions. Another interesting statistic, the personal mobile usage by 61% while working on company data, also addresses the lack of training and the education towards security awareness. The decreased level of security on personal mobile devices increases the vulnerability for the sensitive data.

Phishing examples can be performed by attackers include attachment looking ransomware, where employees easily click and download to their devices or fake links to web pages that can steal sensitive information. The simple but dangerous examples of these attacks easily access the information that should have been protected. Therefore, the article highlights the need of training to ensure security awareness throughout the organization: "Security awareness is not once a year activity, it needs to be an ongoing activity where employees are continually reminded of these threats that are present to identify and report".

The article mentioned: https://www.itsecurityguru.org/2020/04/23/two-thirds-of-remote-workers-given-no-cybersecurity-training-from-employers-in-the-past-year/

In The News

Richard Hertz **says**

SEPTEMBER 29, 2021 AT 7:59 AM

(Edit)

The article I chose this week is about the ongoing importance of measuring and showing value of security awareness training. As practitioners we can be blind to the fact that other people might not be aware of the importance of security awareness. It is 2nd nature to us and therefore sometimes surprising that people don't immediately see the importance of this kind of training. This article talks about a 3 step approach to defining measures inside an organization: 1) Establish a Vision 2) Develop Outcome Driven Measures 3) Link the Operational Outcomes to Business Benefits. I liked the fact that #3 was called out explicitly. If this is not done, then security can be relegated to the level of 'OverHead' which most organizations aggressively seek to minimize. However, shifting the value of security awareness training by showing business benefits changes the conversation!

https://www.cybersecuritydive.com/news/gartner-security-awareness-training/601735/

Where would you look to learn about cybersecurity awareness and training controls?

Where would you look to learn about cybersecurity awareness and training controls?

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

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

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

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(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**				

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

How would you audit these risk controls?

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

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

How would you assess the existence and strength of the AT-2 control ?

NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

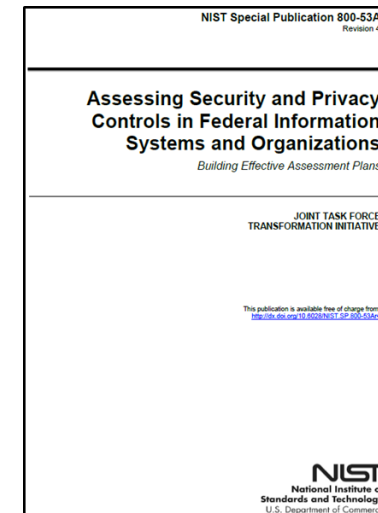JOINT TASK FORCE
TRANSFORMATION INITIATIVE

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

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

...answer:

AT-2	SECURITY AWARENESS TRAINING		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	AT-2(a)	provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users;	
	AT-2(b)	provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes; and	
	AT-2(c)	AT-2(c)[1]	defines the frequency to provide refresher security awareness training thereafter to information system users (including managers, senior executives, and contractors); and
		AT-2(c)[2]	provides refresher security awareness training to information users (including managers, senior executives, and contractors) with the organization-defined frequency.

POTENTIAL ASSESSMENT METHODS AND OBJECTS:

Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records].

Interview: [SELECT FROM: Organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities; organizational personnel comprising the general information system user community].

Test: [SELECT FROM: Automated mechanisms managing security awareness training].

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

How would you assess the existence and strength of the AT-2 (2) control ?

NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

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

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

...answer:

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

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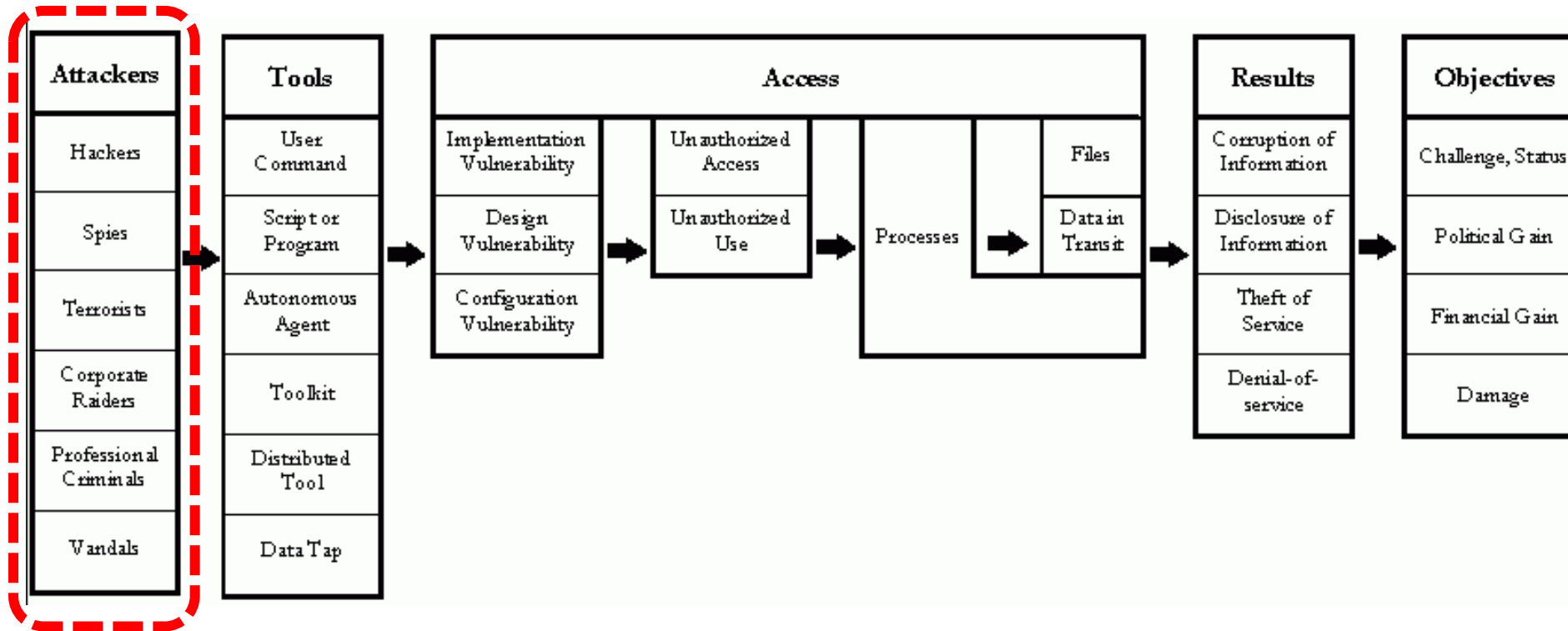
Howard's process-based taxonomy, from Hansman, S. and Hunt, R., 2004, "A taxonomy of network and computer attacks", Computers & Security, page 3, Elsevier Ltd. Cited from Howard, JD, 1997, "An analysis of security incidents on the internet 1989-1995. PhD thesis, Carnegie Mellon University.

The threat landscape….

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

Information Security Threats

Humans

Malicious Attacks
- IP theft
- IT sabotage
- Fraud
- Espionage

Non-Malicious Mistakes

Outsiders
- Hackers
- Crackers
- Social engineers
- …

Insiders
- Disgruntled employees
- …

Employee Mistakes
- Ignorance
- …

Intentional Rule Breaking
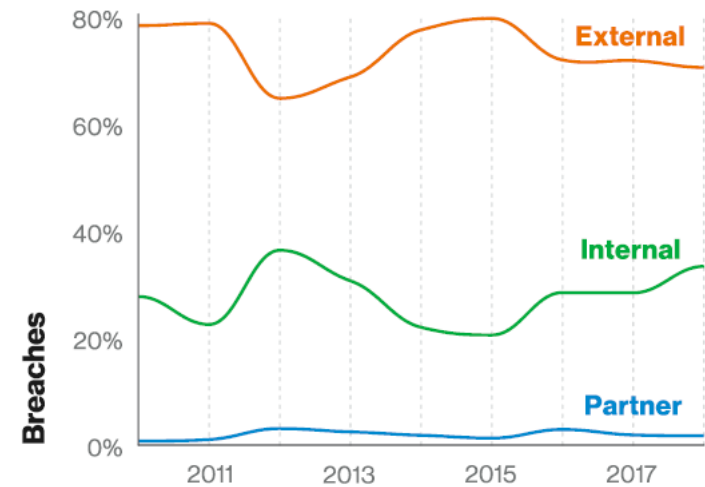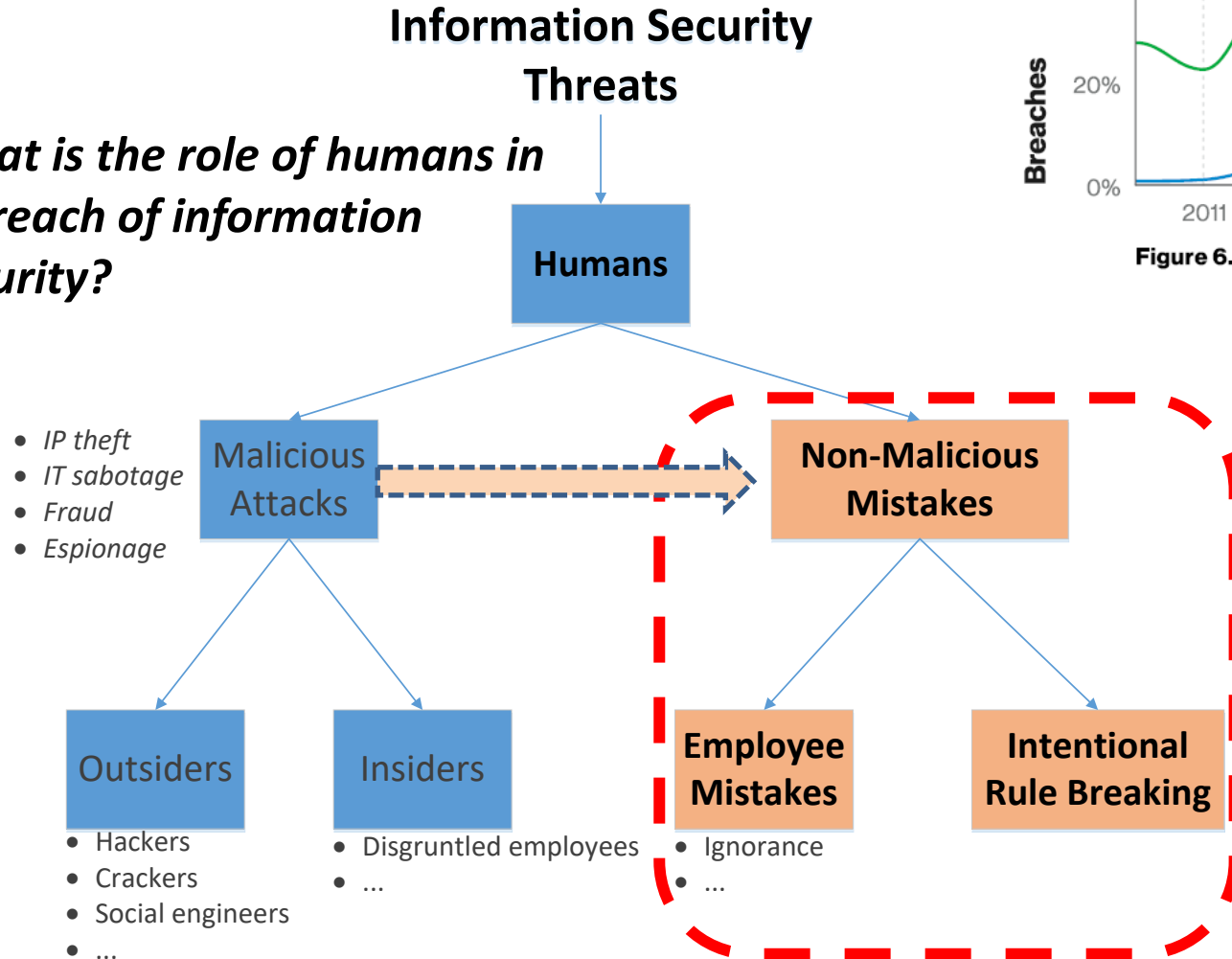
Figure 6. Threat actors in breaches over time

2019 Data Breach Investigations Report

verizon
business ready

What roles do employees play in these attack chains

2019 Data Breach Investigations Report

verizon
business ready

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

Figure 30. Attack chain by final attribute compromised[12] (n=941)
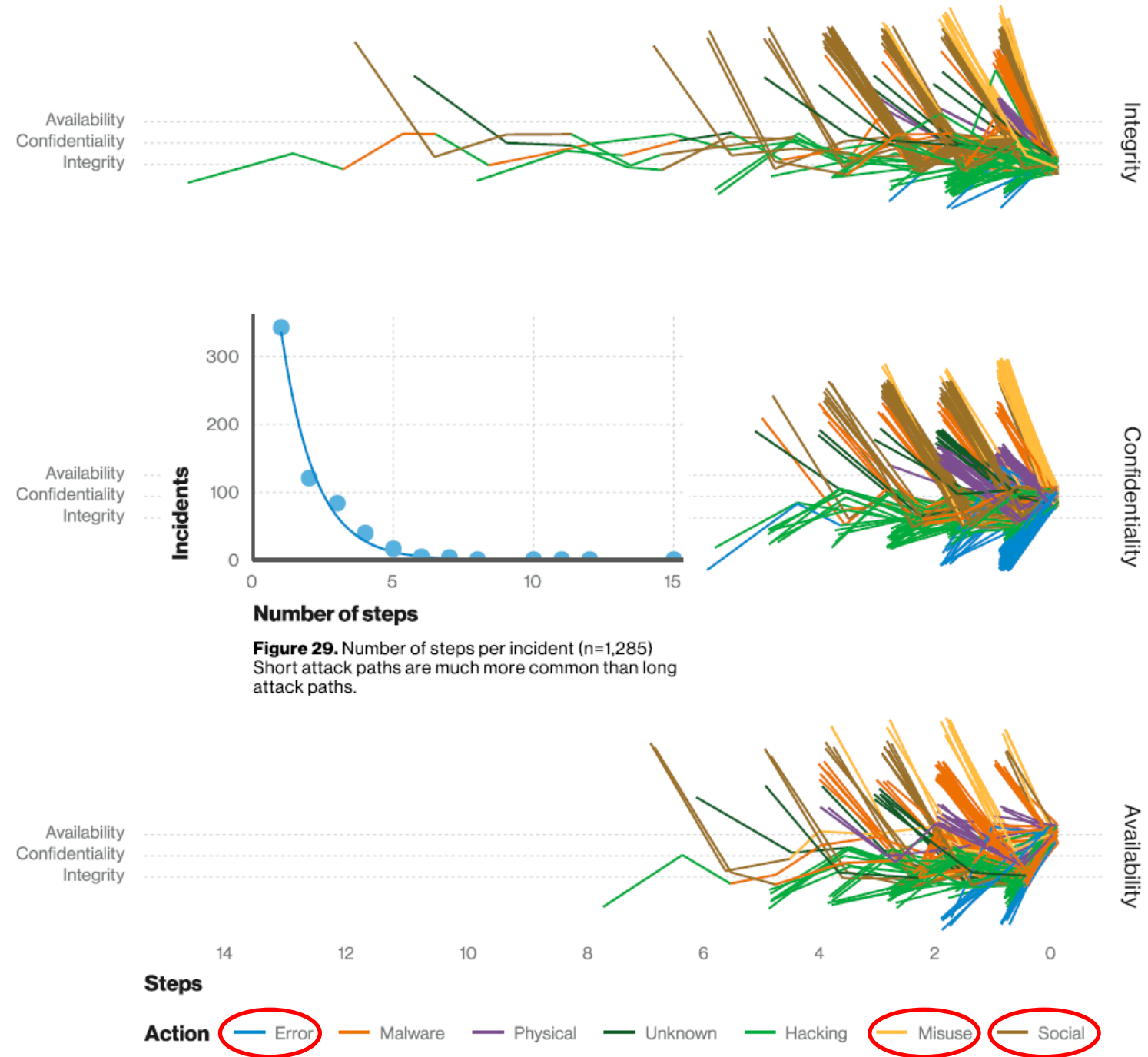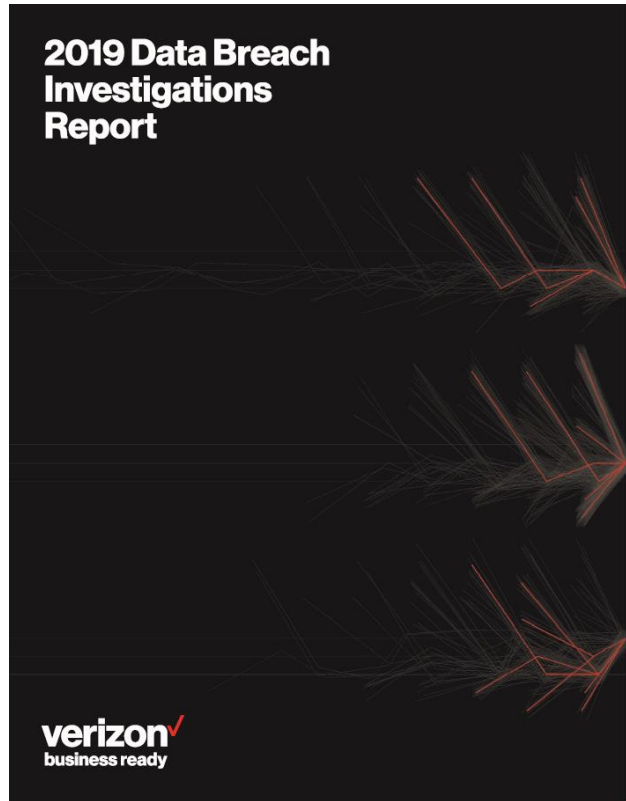
Top Threats 2019-2020	Assessed Trends	Change in Ranking
1 Malware ↗	----	----
2 Web-based Attacks ↗	----	↗
3 Phishing ↗	↗	↗
4 Web application attacks ↗	----	↙
5 Spam ↗	↙	↗
6 Denial of service ↗	↙	↙
7 Identity theft ↗	↗	↗
8 Data breaches ↗	----	----
9 Insider threat ↗	↗	----
10 Botnets ↗	↙	↙
11 Physical manipulation, damage, theft and loss ↗	----	↙
12 Information leakage ↗	↗	↙
13 Ransomware ↗	↗	↗
14 Cyberespionage ↗	↙	↗
15 Crytojacking ↗	↙	↙

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

From January 2019 to April 2020

The year in review

ENISA Threat Landscape

European Union Agency for Cybersecurity (ENISA)

In which of these threats are humans the vulnerability?

Employee Risk

- [Ponemon Institute](#) (2018) surveyed 1,000 small and medium-sized business owners, found negligent employees or contractors caused 60% of the data breaches

    - Employee training and stringent security protocols are necessary to mitigate risk of malicious insiders, otherwise danger of data breach remains high

- [Ponemon survey](#) (2018) of 612 CISOs found that 70% consider the "lack of competent in-house staff" as their top concern in 2018

Employee Risk

Verizon 2019 Data Breach Investigation Report

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

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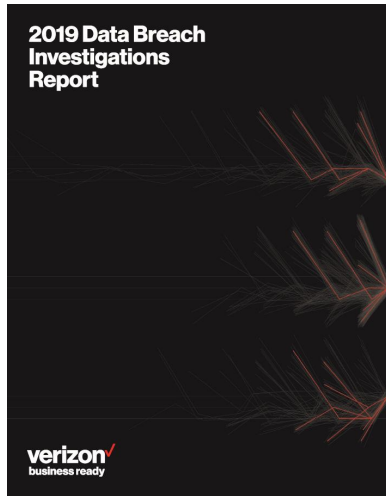
Employee Risk

Malware delivery methods

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

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

2019 Data Breach Investigations Report

verizon√
business ready

File Type

45%	**26%**	**22%**
Office doc	Windows app	other

100%

75%

50%

25%

0%
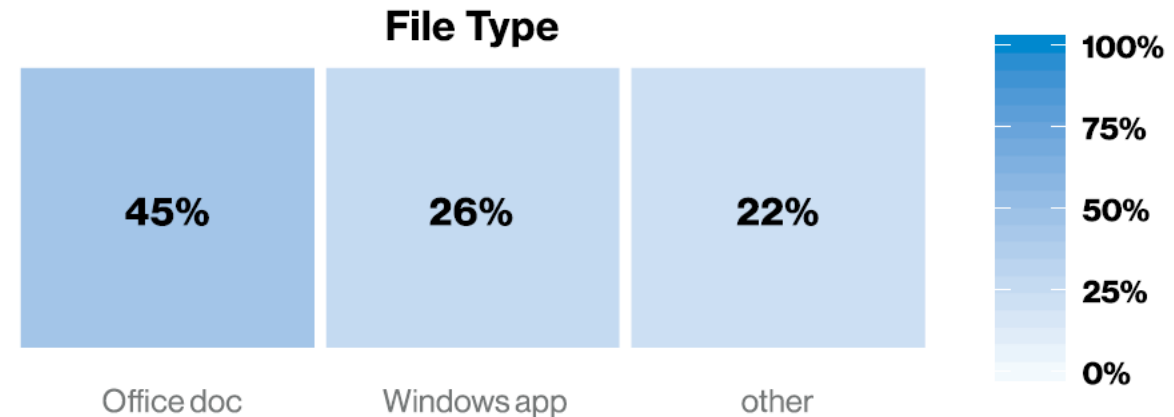
- 37% of breaches stole or used credentials

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

2020 Data Breach Investigations Report

verizon

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

October 2020

Ponemon Institute © 2020 Research Report

KEEPER
Cybersecurity Starts Here

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

- A lack of physical security in the teleworker's work space — 47%
- Teleworkers' devices become infected with malware — 32%
- Criminals could gain control of teleworkers' devices to steal sensitive and confidential data — 24%
- The inability to secure communications on external networks outside your organization's control — 23%
- The difficulty in securing your organization's network — 20%
- Criminals could leverage the devices to gain access to the enterprise network — 17%
- Phishing and social engineering scams directed at teleworkers — 15%
- Teleworkers lose or have their devices stolen — 12%
- The difficulty in securing external access to internal-only resources — 8%
- Other — 1%

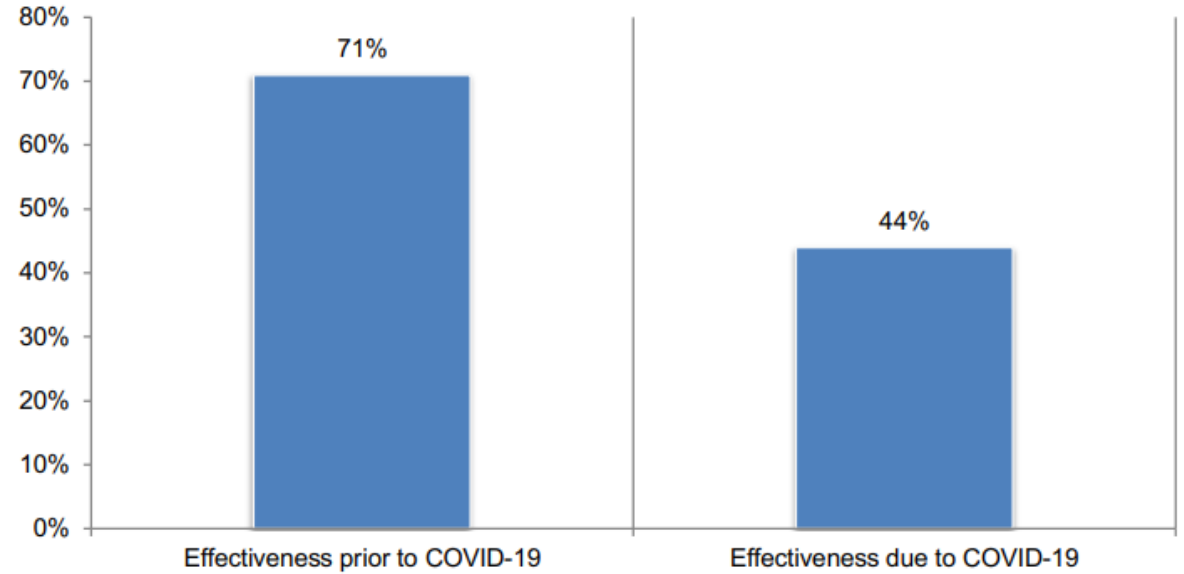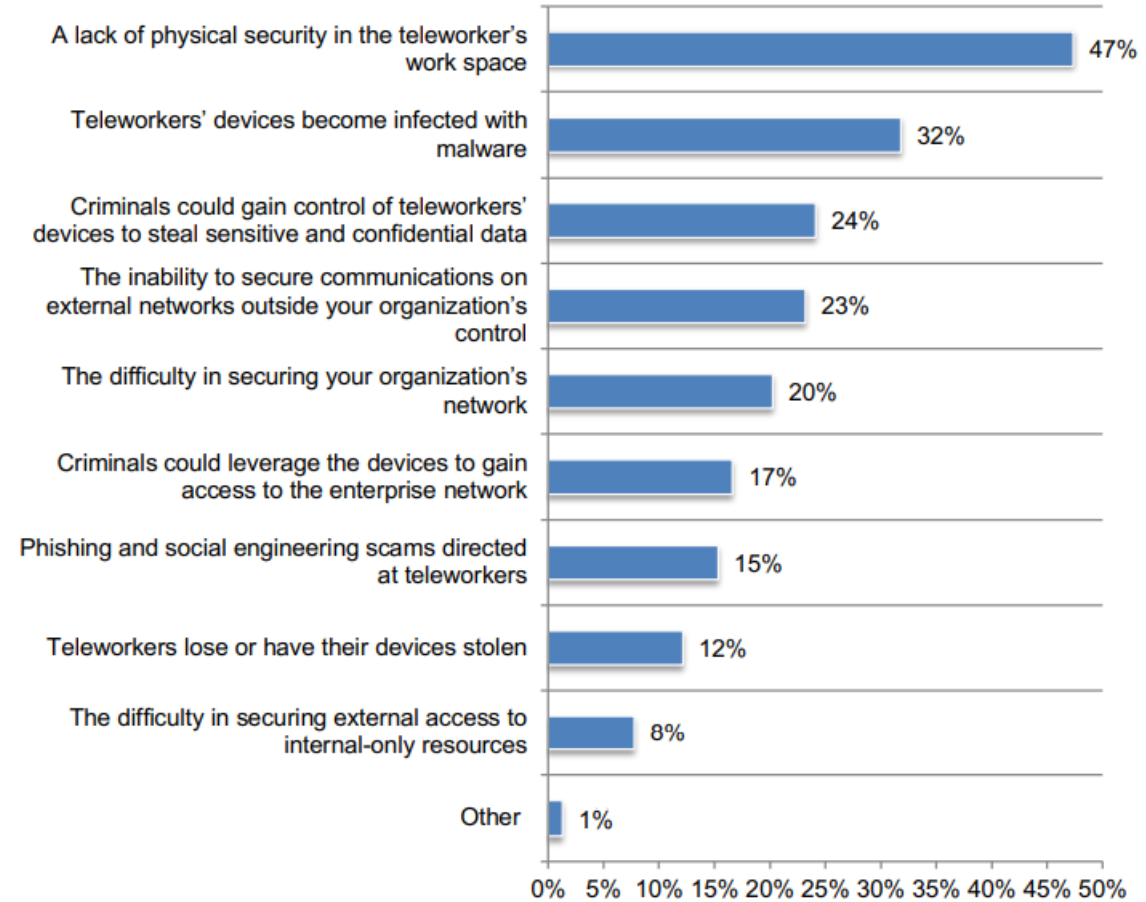**Cybersecurity in the Remote Work Era:**

A Global Risk Report

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

October 2020

Ponemon Institute © 2020 Research Report

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

Challenge	Percentage
Insufficient budget (money)	44%
No understanding how to protect against cyberattacks	42%
Insufficient enabling security technologies	27%
Lack of clear leadership	25%
Lack of in-house expertise	24%
Insufficient personnel	19%
Management does not see teleworking causing security risks	18%
Other	2%
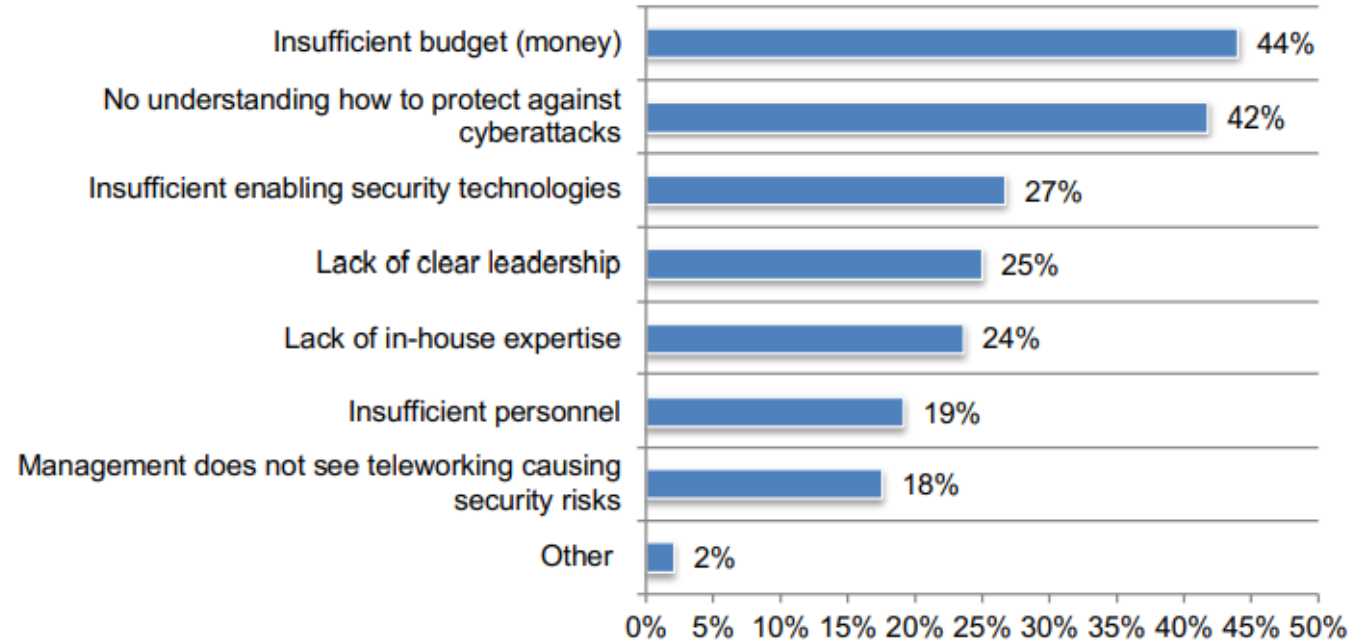
Why is teaching security awareness essential ?

- We have a culture of trust that can be taken advantage of with dubious intent

- Most people feel security is not part of their job

- People underestimate the value of information

- Security technologies give people a false sense of protection from attack

Non-malicious insider threat

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

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

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

Major characteristic is '*failure in human performance*'

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

The Unintentional Insider threat

from an ad for…

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

"You spelled 'confidential' wrong."

How would you characterize insiders' information security mistakes

- **Ignorant**
  - An unintentional accident

- **Negligent**
  - Willingly ignores policy to make things easier

- **Well meaning**
  - Prioritizes completing work and "getting 'er done" takes over following policy

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

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

What are examples of insiders' accidents ?

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

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

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

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

Utah Medicaid contractor loses job over data breach

By Kirsten Stewart The Salt Lake Tribune

Published January 17, 2013 5:26 pm

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

"Terrific employee":

- Account Manager handling health data for Utah

- Employee had trouble uploading a file requested by State Health Dept.

- Copied 6,000 medical records to USB drive

- Lost the USB drive, and reported the issue

- CEO admits the employee probably didn't even know she was breaking policy
  - this makes it accidental i.e. "well meaning…"
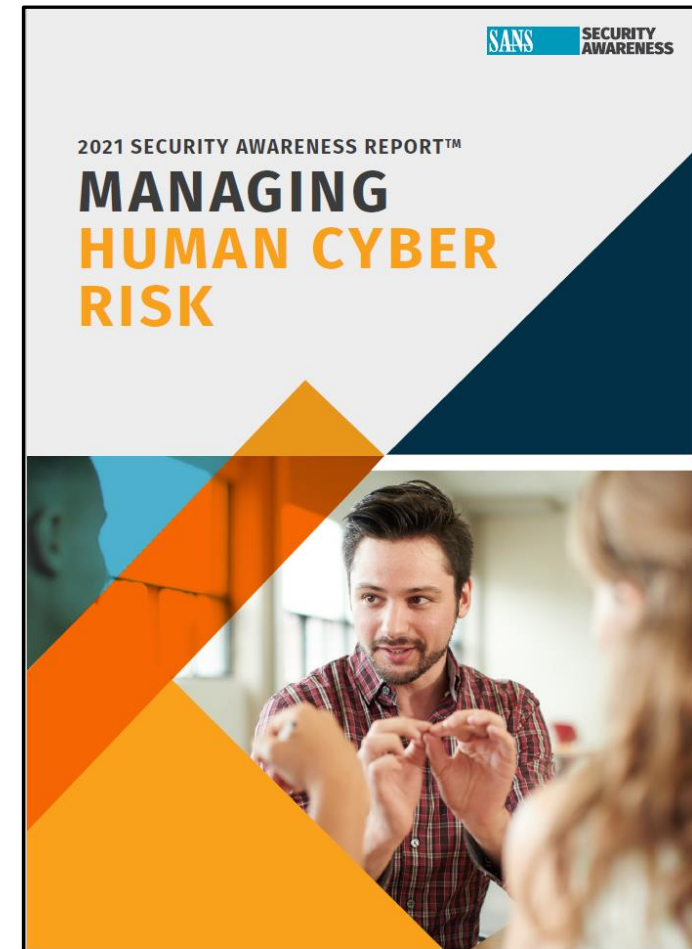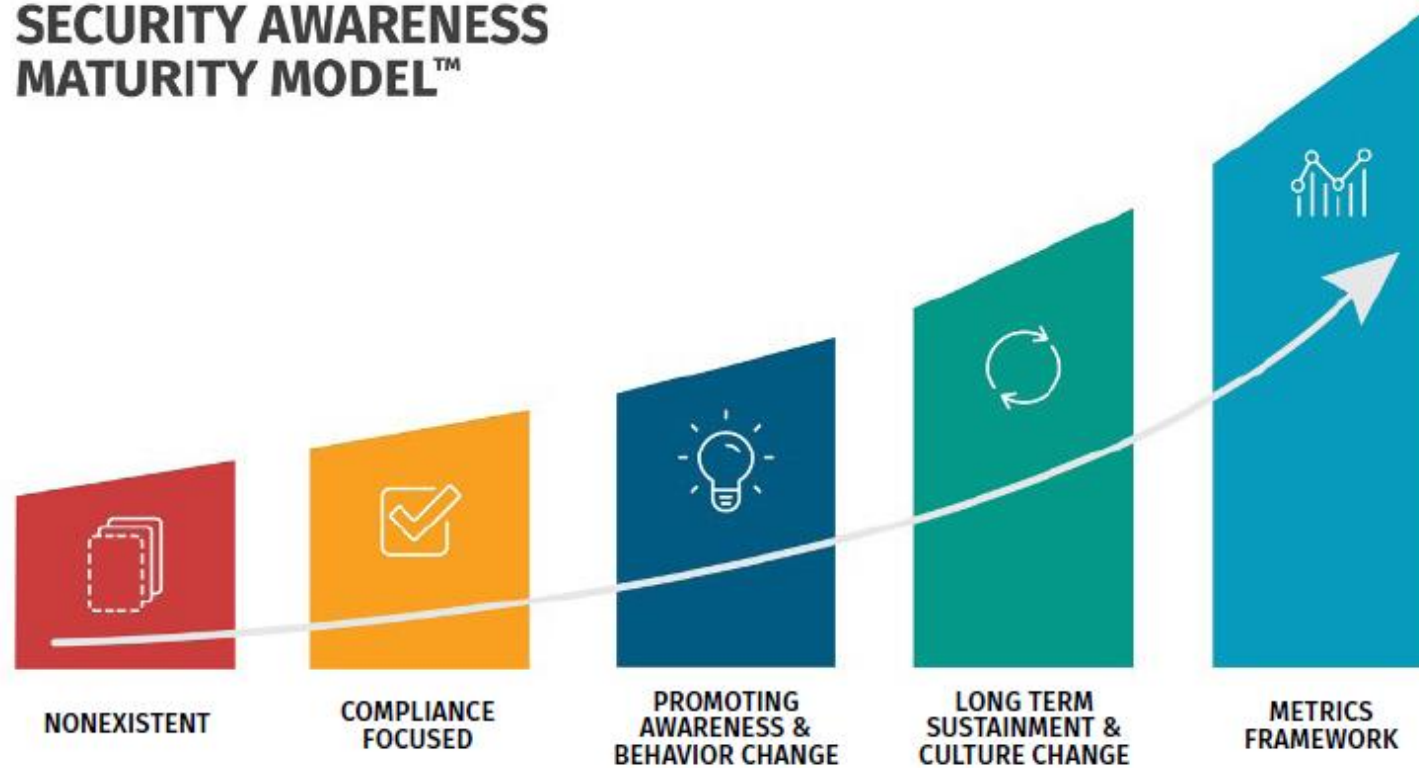
Auditing a Security Awareness Training control

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

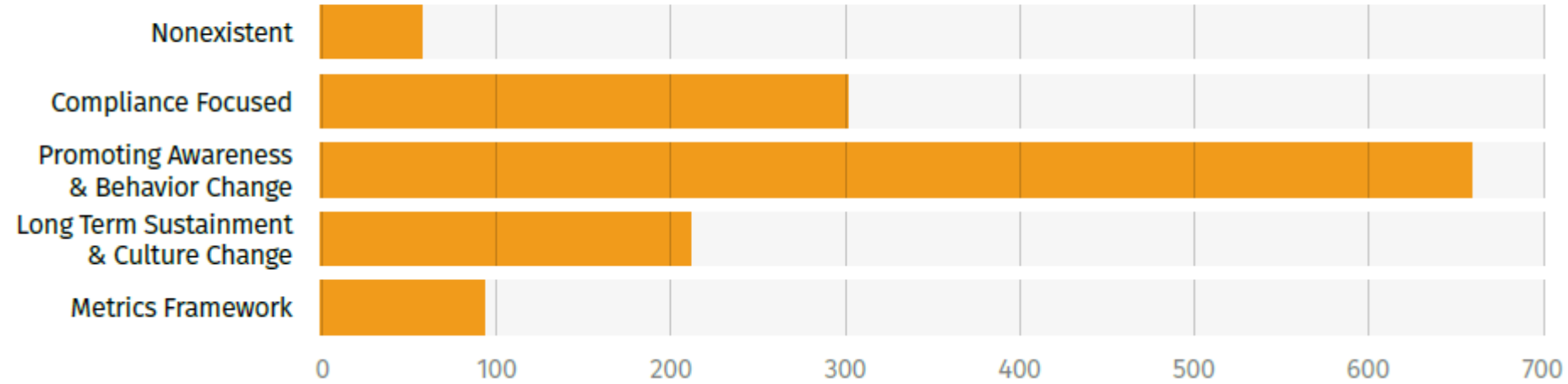| AT-2(2)	SECURITY AWARENESS TRAINING | *INSIDER THREAT*
	ASSESSMENT OBJECTIVE: *Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [SELECT FROM: Security awareness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

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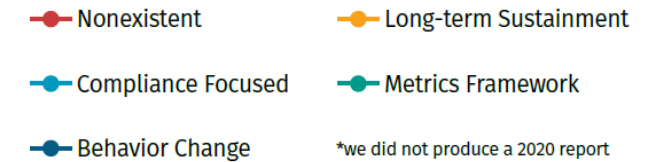

SECURITY AWARENESS MATURITY MODEL™

NONEXISTENT | COMPLIANCE FOCUSED | PROMOTING AWARENESS & BEHAVIOR CHANGE | LONG TERM SUSTAINMENT & CULTURE CHANGE | METRICS FRAMEWORK

2021 SECURITY AWARENESS REPORT™
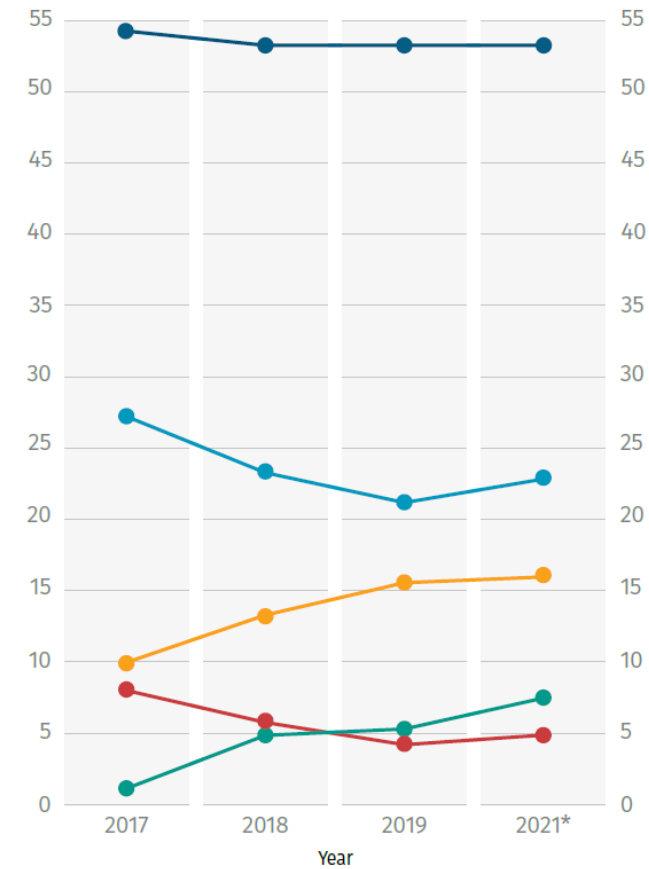MANAGING HUMAN CYBER RISK

SANS SECURITY AWARENESS

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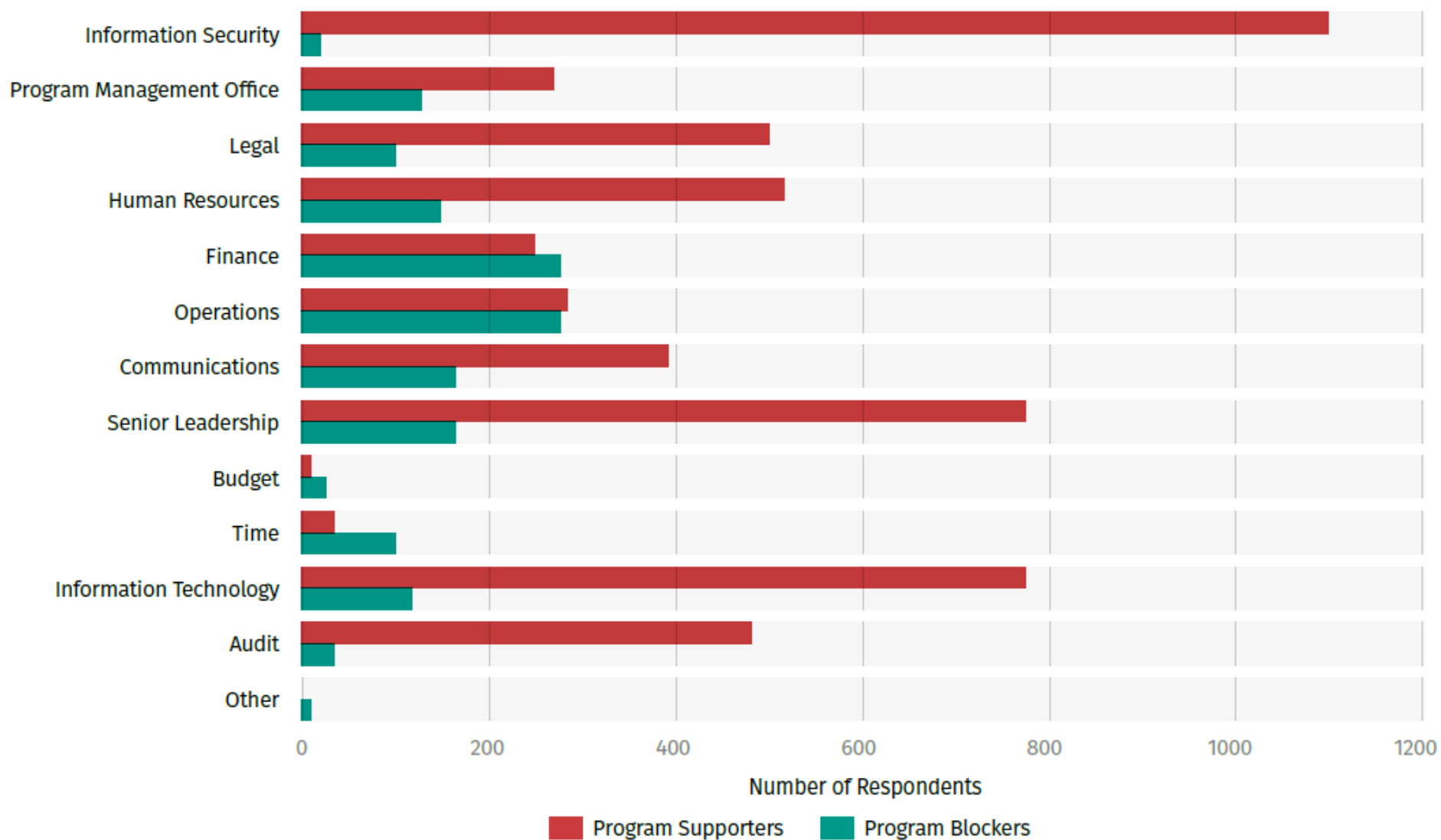
Benchmarking Maturity Levels

Program Maturity Over Time

Reported Program Blockers and Supporters

GAINING LEADERSHIP SUPPORT

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

Support Level

- I have no support
- I have less support than I need
- I have the support I need
- I have more support than I need

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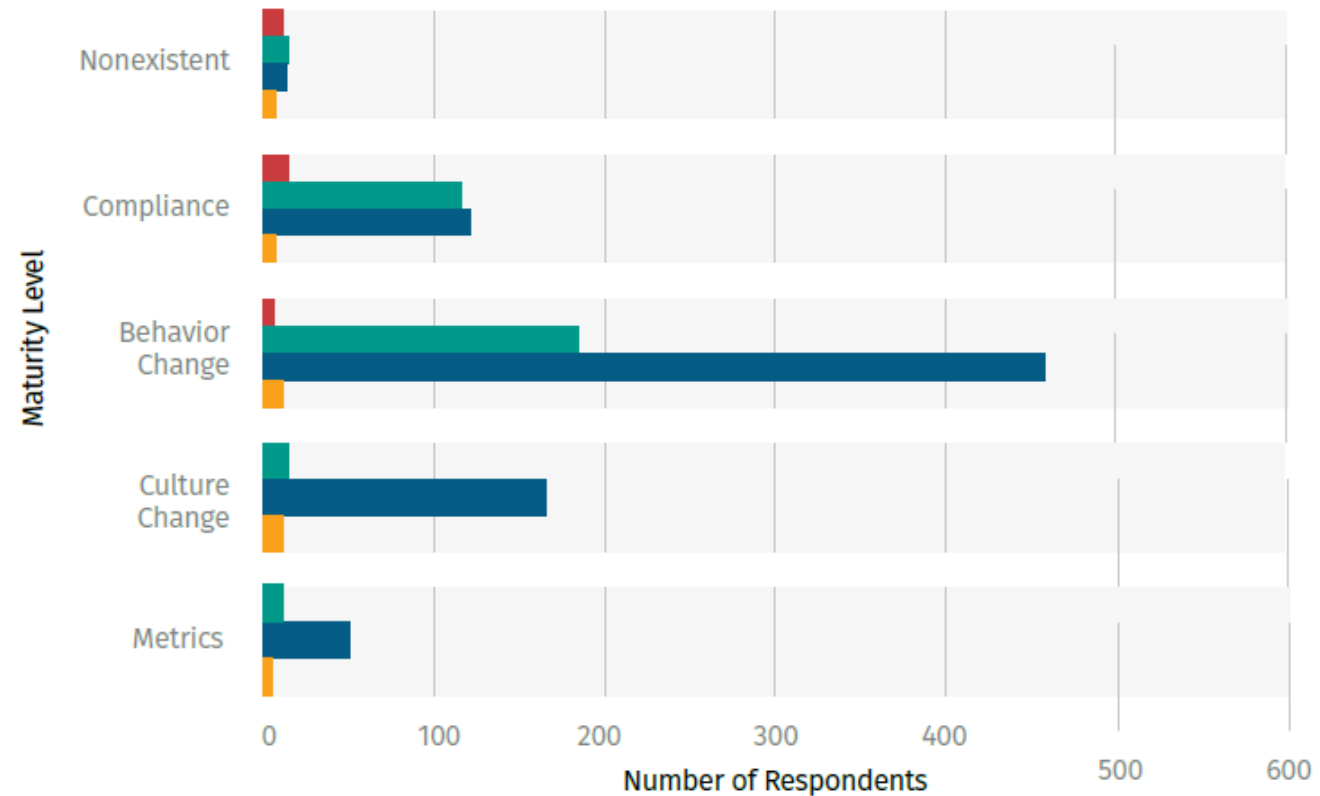
Top Reported Program Challenges
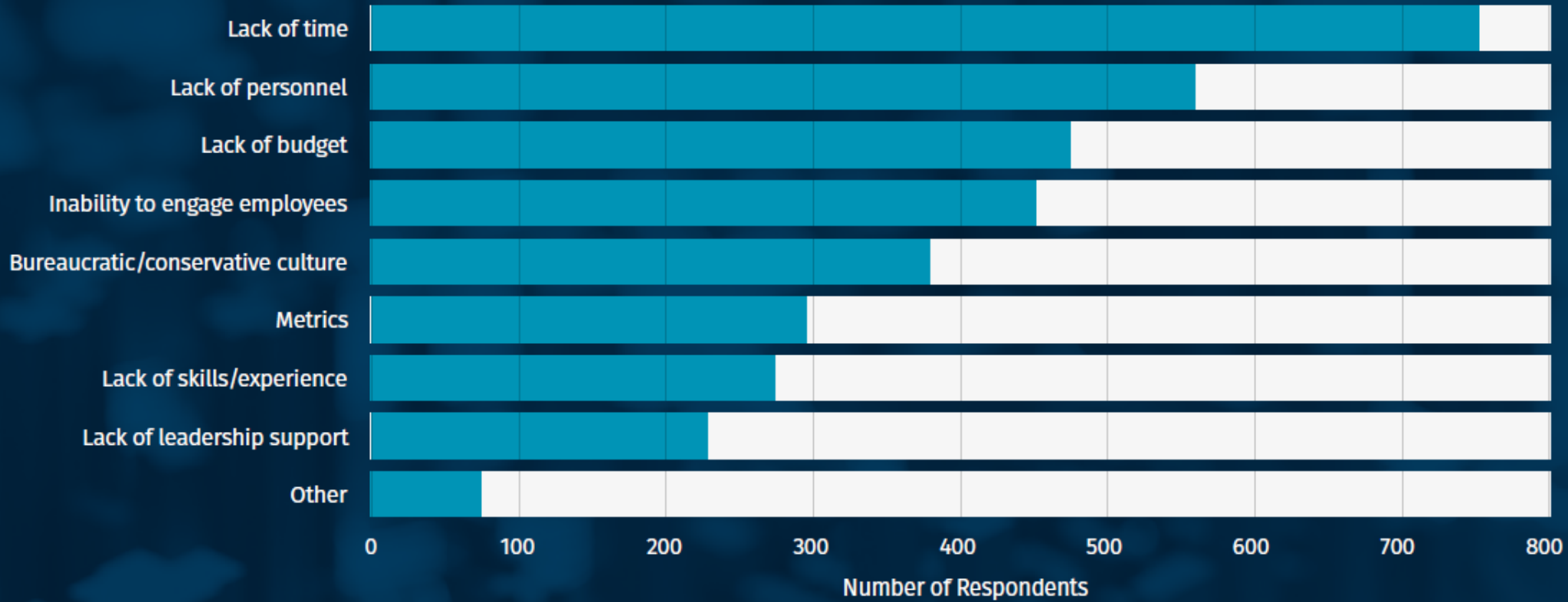
Over 80% of security awareness professionals reported that they spend half or less of their time on awareness, indicating far too often that security awareness is a part-time effort.

Percentage of Time Spent on Security Awareness

Average Number of FTEs by Maturity Level

Average Number of FTEs by Org Size

SANS SECURITY AWARENESS

Summary of Key Action Items

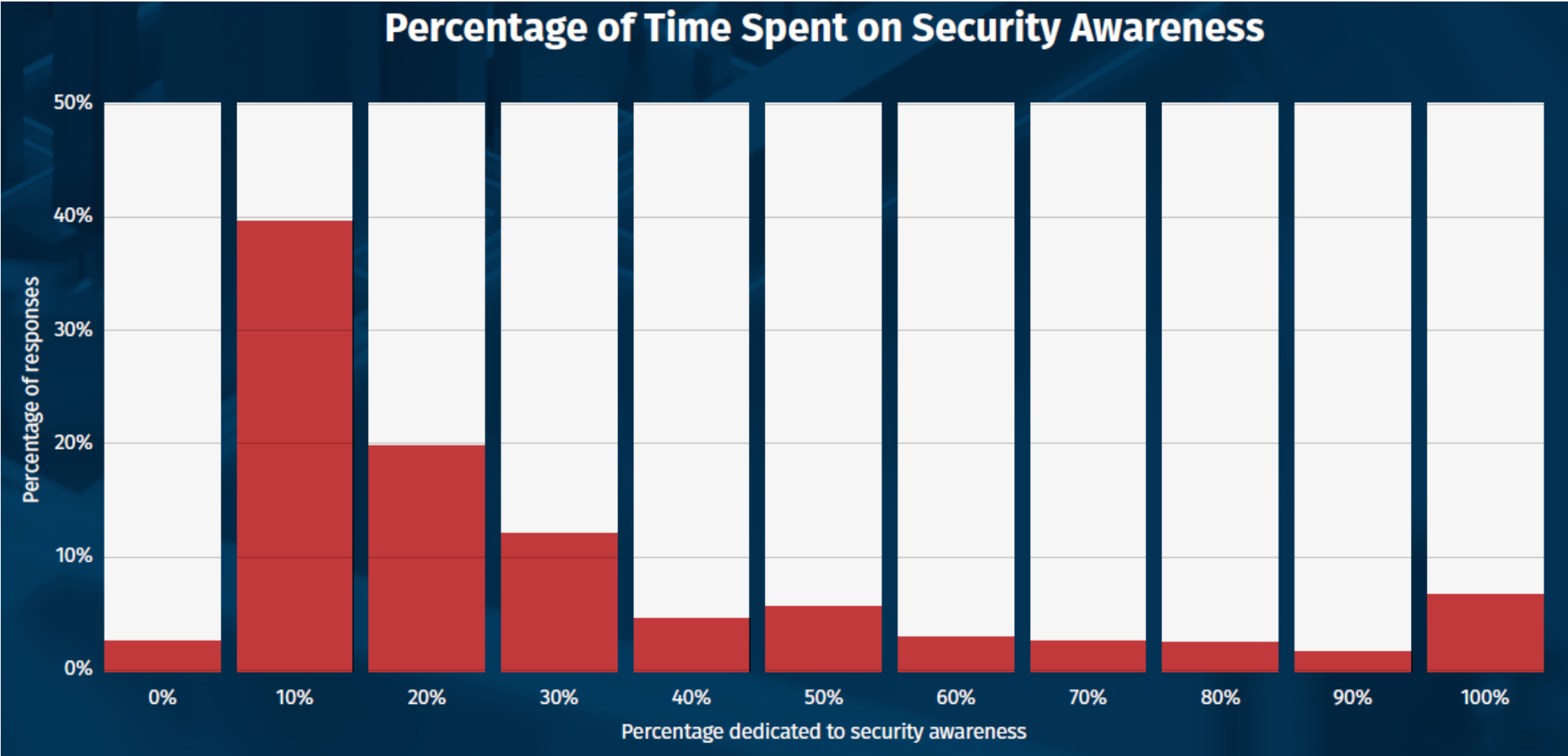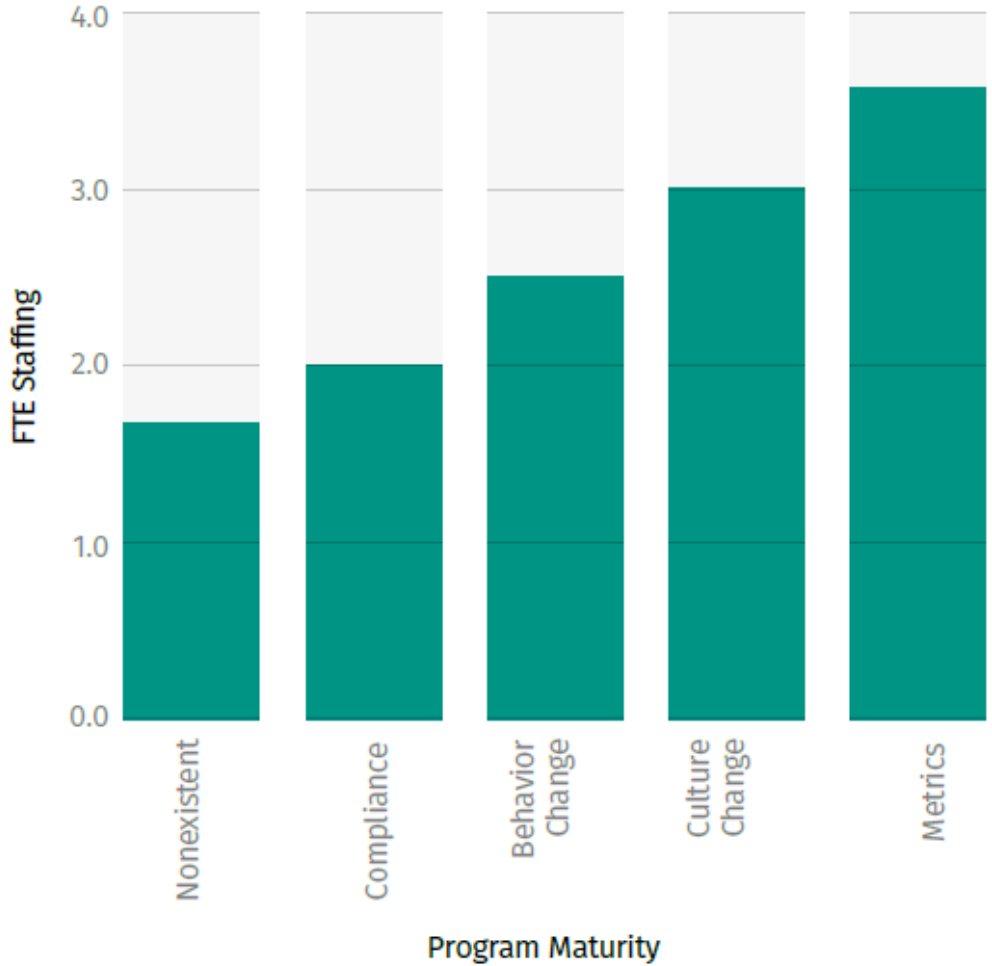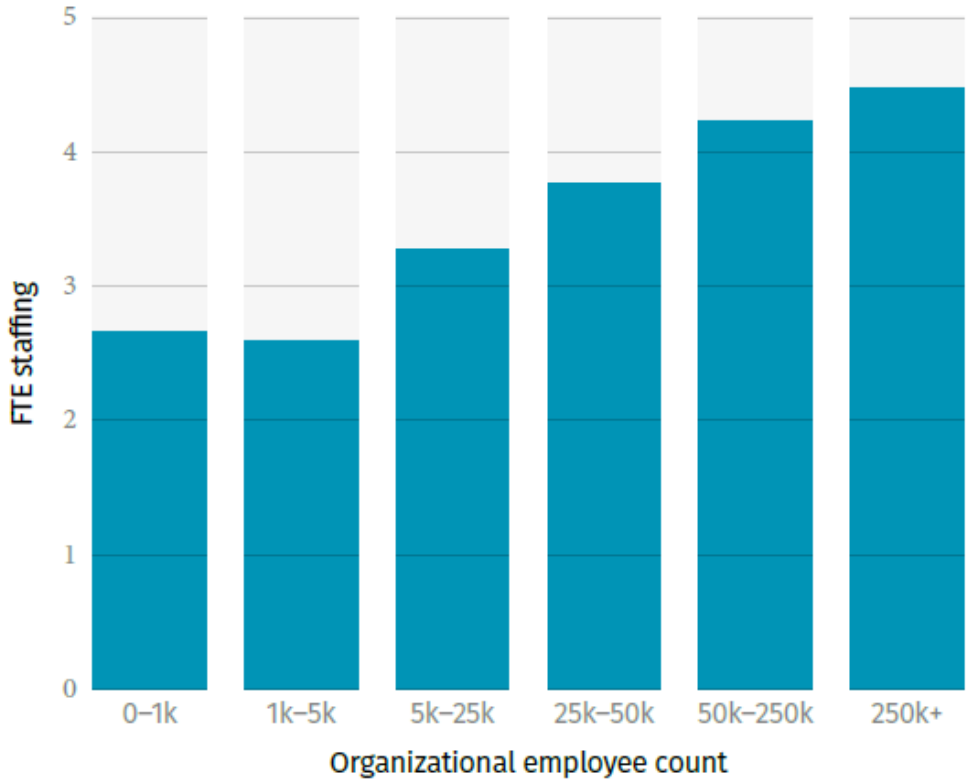- **Have the Right People:** You need 2.5 FTEs to begin changing behavior at an organizational level.

  > **To achieve a truly mature program, including a strong metrics framework, you will need at least 3.5 FTEs.**

  FTE numbers may vary depending on organizational size, structure, and requirements.

- **Provide the Right Title:** Demonstrate organizational commitment to the program, not only by having someone dedicated full-time but also by ensuring they have a title that aligns with the program's goals. In other words, have a title that is focused on managing human risk.

- **Ensure Leadership Support:** Pressure is one of the most effective means to obtain leadership support. Demonstrate to your leadership how other organizations in your industry have mature awareness programs and continue to invest in them.

- **Encourage Partnerships:** Build partnerships and collaborate with others in your organization. This is especially important for any key departments that are blockers, such as Finance or Operations. Get key stakeholders involved in the planning process from the beginning.

- **Buy Time:** If you have the budget, use it to buy yourself time. For example, buy or license materials rather than create your own.

- **Know Your Bias:**

  > **If you are a technical or security expert, make sure you work with others to create clear messaging.**

  Your expertise is a plus as long as you pay careful attention to how it contributes to your program.

MIS 5206 Protecting Information Assets

Summary of Key Action Items

- **Improve Communication and Engagement Skills:** Be sure you have someone on your awareness team who has the skills required for effective communication and engagement.

- **Seek out a Champion:** Find a strong champion within leadership. Have that leader help you better understand certain blockers, communicate the value of your program to other leaders, or help you craft your message in the language that business leaders understand and act on.

- **Improve Perception:** Focus and speak in terms of managing human risk. Human risk is far more aligned with most organizations' strategic security priorities, and it is far more likely to gain leadership buy-in and resonate with a security team.

  ## Identify top human risks and the key behaviors that manage those risks.

  Demonstrate how you can better support the security team with security policies, processes, and priorities. Measure key strategic security metrics that leadership cares about.

Summary of Key Action Items

2021 SECURITY AWARENESS REPORT™
MANAGING HUMAN CYBER RISK

- **Take Security Training:** Review Appendix B: Career Development for Security Awareness, Engagement, and Culture Professionals.

> **Security training will provide you a better understanding of risks and the different technologies, frameworks and approaches to managing them, helping build both your credibility and value.**

APPENDIX B: CAREER DEVELOPMENT FOR SECURITY AWARENESS PROFESSIONALS

One of the key takeaways from the 2021 report is that your compensation is in part driven by your training and skills, including your understanding of key security topics and the technologies involved. Rightly or wrongly, technical staff are often perceived as more valuable, and improving your technical skills can improve your ability to interact with your technical colleagues. As such, based on the data and findings we have defined a training path to help develop the skills you need to be more successful and be compensated adequately.

WHERE TO START

If you are new to the world of information security and/or security awareness, or haven't had the chance yet, the very first SANS course you may want to start with is:

- **MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program:** This two-day class lays the foundation of security awareness, managing human risk and ultimately changing organization behavior. For those of you new to security, you will learn concepts like risk, risk management, and risk analysis. For those of you new to communications and engagement, you will learn key concepts such as the AIDA model, Start with Why, Curse of Knowledge, and other models and principles. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you will implement... return to your organization.

- **SEC301: Introduction to...** your security knowledge... Instruction on critical inf... are fundamental to cybe... to cybersecurity. It... technology to the basi... and networks, security p... cryptographic principles,... malware, wireless securi... security technologies, w... backups, virtual machine... All topics are covered at... hands-on, step-by-step t... you to grasp all the infor... some of the topics are n... world cybersecurity fund... foundation of your caree... years to come.

WHAT NEXT

Once you have the basics down and want to develop yourself and your career, you may need to develop your security expertise if you do not have a technical or security background. Understanding the fundamentals will not only help you better understand the risks, but also the behaviors that manage those risks and empower you to more effectively communicate with your security team and security leadership. There are two different five-day courses to consider at this stage in your career. Each has its advantages, depending on what you hope to achieve.

- **MGT512: Security Leadership Essentials For Managers:** This course empowers you to become an effective security mar... speed quickly on inform... terminology. You won't ju... will learn how to manag... this goal, MGT512 covers... network, host, applicatio... covered in conjunction... that address the overall... includes governance and... on protecting, detecting,... issues.

Not sure which one of these two courses to take? If you are looking for more of a high-level or management perspective to the world of information security, we recommend MGT512. If you want a more hands-on, technical introduction to the tools and technology of cybersecurity, then we recommend SEC301.

INTERMEDIATE LEVEL

Once you have 2-4 years of experience in security awareness and feel confident in the concepts of both cybersecurity and organizational behavior, MGT521 is what we recommend next.

- **MGT521: Driving Cybersecurity Change – Establishing a Culture of Protect, Detect and Respond:** Cybersecurity is no longer just about technology - it is ultimately about organizational change. Change in not only how people think about security but what they prioritize and how they act, from the Board of Directors on down. Organizational change is a field of management study that enables organizations to analyze, plan, and then improve their operations and structures by focusing on people and culture. SANS MGT521 will teach leaders how to leverage the principles of organizational change, enabling them to develop, maintain and measure a security-driven culture. Through hands-on, real-world instruction and a series of interactive labs and exercises in which you will apply the concepts of organizational change to a variety of

...different security initiatives, you will quickly learn how to embed cybersecurity into your organizational culture.

ADVANCED LEVEL

Once you have 5-7 years of experience and want to truly develop your security leadership skills, consider SANS MGT514. This will walk you through the strategic planning process and challenges CISOs face. Many people consider this the "CISO Course", that helps develop new and experienced Chief Information Security Officers to become better security leaders. By better understanding CISO challenges, priorities and concerns, you can more effectively collaborate with them and communicate in their terms and language.

- **MGT514: Security Strategic Planning, Policy, and Leadership:** This course gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create an effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

By actively growing your skills and knowledge, you can not only become a more effective leader, but also dramatically improve and broaden your career opportunities.

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

What should be in an information security training course ?

- Create a course outline of topics

- Prioritize the topics for teaching the course

Training courses examples...

Tip #3: Explain to the employees that while you make the best effort to secure company infrastructure, a system is only as secure as the weakest link

- ▶ You don't want them to just comply, you want them to cooperate

- ▶ You can't create a policy sophisticated enough to cover all possible vectors of attack

- ▶ You can't totally dehumanize humans. Humans have weaknesses and make mistakes.

KASPERSKY lab

Training course content example

A. Physical security

B. Desktop security

C. Wireless Networks and Security

D. **Password security**

E. Phishing

F. Hoaxes

G. Malware

   1. Viruses

   2. Worms

   3. Trojans

   4. Spyware and Adware

H. File sharing and copyright

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

Training course content example

A. Password safety and security

B. Email safety and security

C. Desktop security

D. FERPA Issues (i.e. student information security)

E. Acceptable Use Policy

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

Training course example...

Password safety and security

- 80% of hacking related data breaches involve Brute force or the use of compromised credentials (login and password)
- 37% of all breaches involve the use of stolen credentials

  2020 Verizon Data Breach Investigations Report

- Security policies need to cover both computer <u>and</u> voice mail passwords
- Every employee should be instructed in how to devise a difficult-to-guess password

MIS 5206 Protecting Information Assets

How Secure Is My Password?
✓ The #1 Password Strength Tool. Trusted and used by millions.

......

It would take a computer about
4 hundred milliseconds
to crack your password

HOW SECURE IS MY PASSWORD?

••••••••

It would take a computer about
22 MINUTES
to crack your password

How Secure My Password
Test the strength of my password

DonDiego45&^67

It would take a computer about
816 million years
to crack your password

Training course content

Email and Voicemail

- Email usage policy, including the safeguards to prevent malicious code attacks including viruses, worms, and Trojan Horses

- Best security practices of voice mail usage

Phishing Prevention-The 100% rules!

- Never click a link in an email
- Never open unexpected attachments
- Never provide information, no matter how innocuous it may seem, to unsolicited phone callers, visitors or email requests
- Never agree to an unsolicited remote control session (such as WebEx, GoToMeeting, LogMeIn)
- Your best defense: "Can I call you back?"

KASPERSKY lab

Training course content

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

Handling sensitive information

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

Creating a Security Aware Organization

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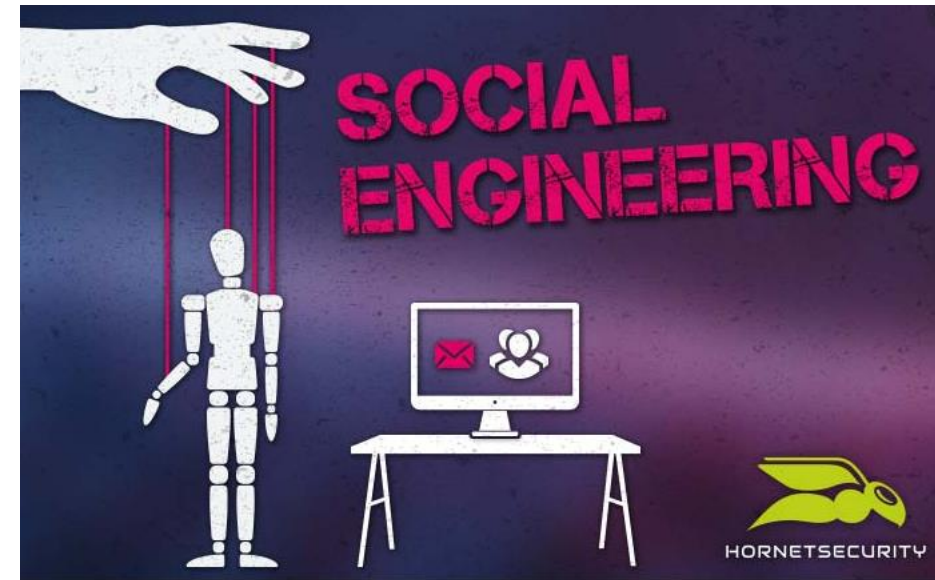
What is social engineering?

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

▶ A lot of cyberincidents start with a phone conversation with someone who poses as a co-worker and builds his understanding of company internal structure and operations by asking innocent questions

▶ A cybercriminal exploiting social weaknesses almost never looks like one

KASPERSKY

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

3 BASIC TYPES OF TACTICS

IN-PERSON   PHONE   DIGITAL

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

The clever **manipulation** of the natural human tendency to trust!

What is "just in time training?"

"Just in time training…"

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

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

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

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

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

"Just in time training…"

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

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

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

Test Taking Tip

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

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

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

[Quiz](#) and [Solutions](#)

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

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

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

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

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. <mark>Discontinuing activities that introduce risk</mark>
   b. Identifying assets
   c. Identifying threats
   d. Analyzing risk in order of cost or criticality

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

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

Agenda

✓ In The News

✓ Awareness and Training InfoSec Controls

✓ Creating a Security Aware Organization

  ✓ Control inventory baselines

  ✓ The Threat landscape

  ✓ Employee risk

  ✓ Training course content (examples)

✓ Test Taking Tip

✓ Quiz

Protecting Information Assets
- Unit# 5 -

Creating a Security Aware Organization