

Information Systems Integration

MIS 4596

Information Security in Organizations

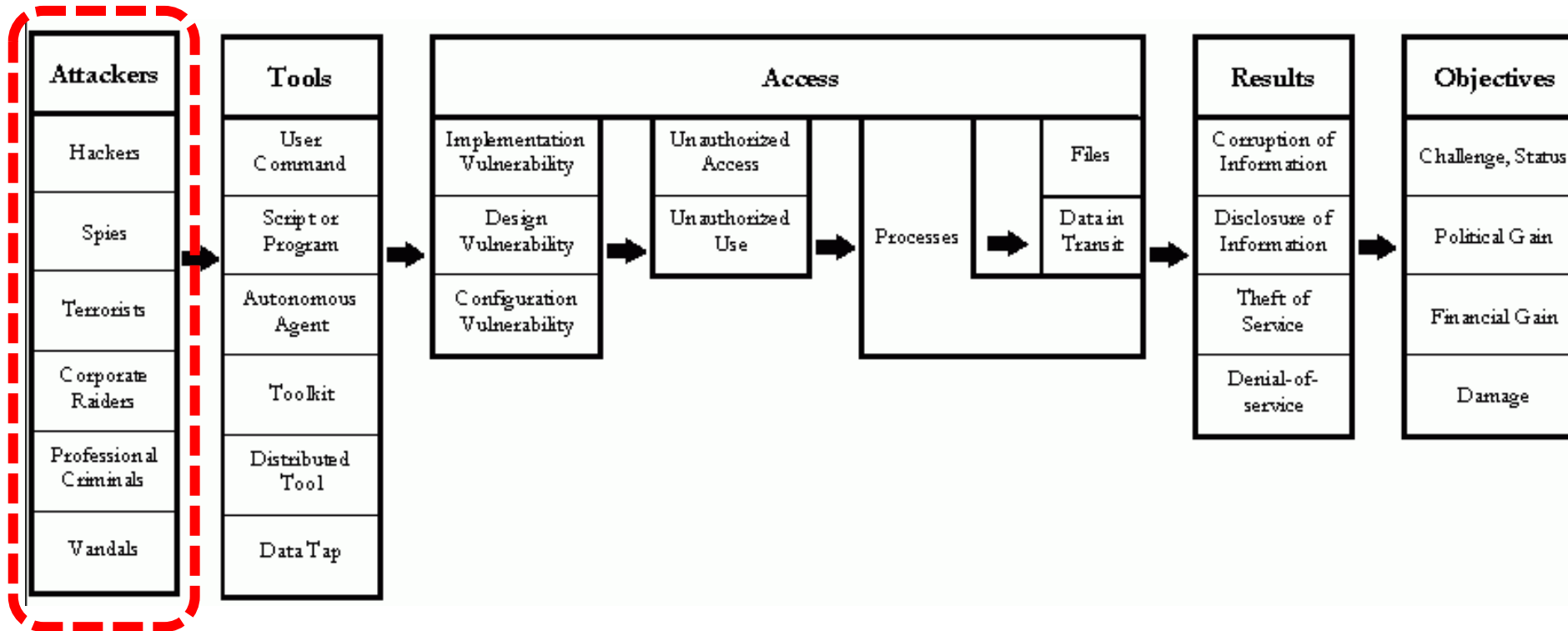
Unit #6

Agenda

- Human element of cyber security
- Employee risk
- Cyber Security Employee Awareness and Training Risk Controls
- Evolution of Organizations' Security Awareness and Training Programs
- Training course content examples

What is in this picture ?

What is missing from this diagram?



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

The threat landscape....

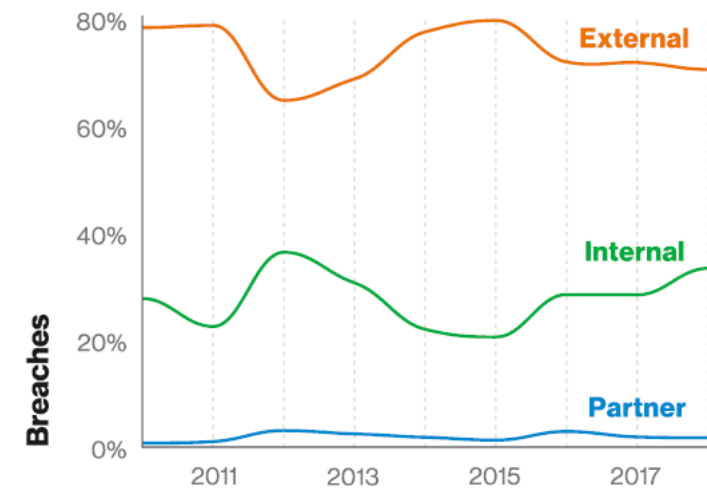
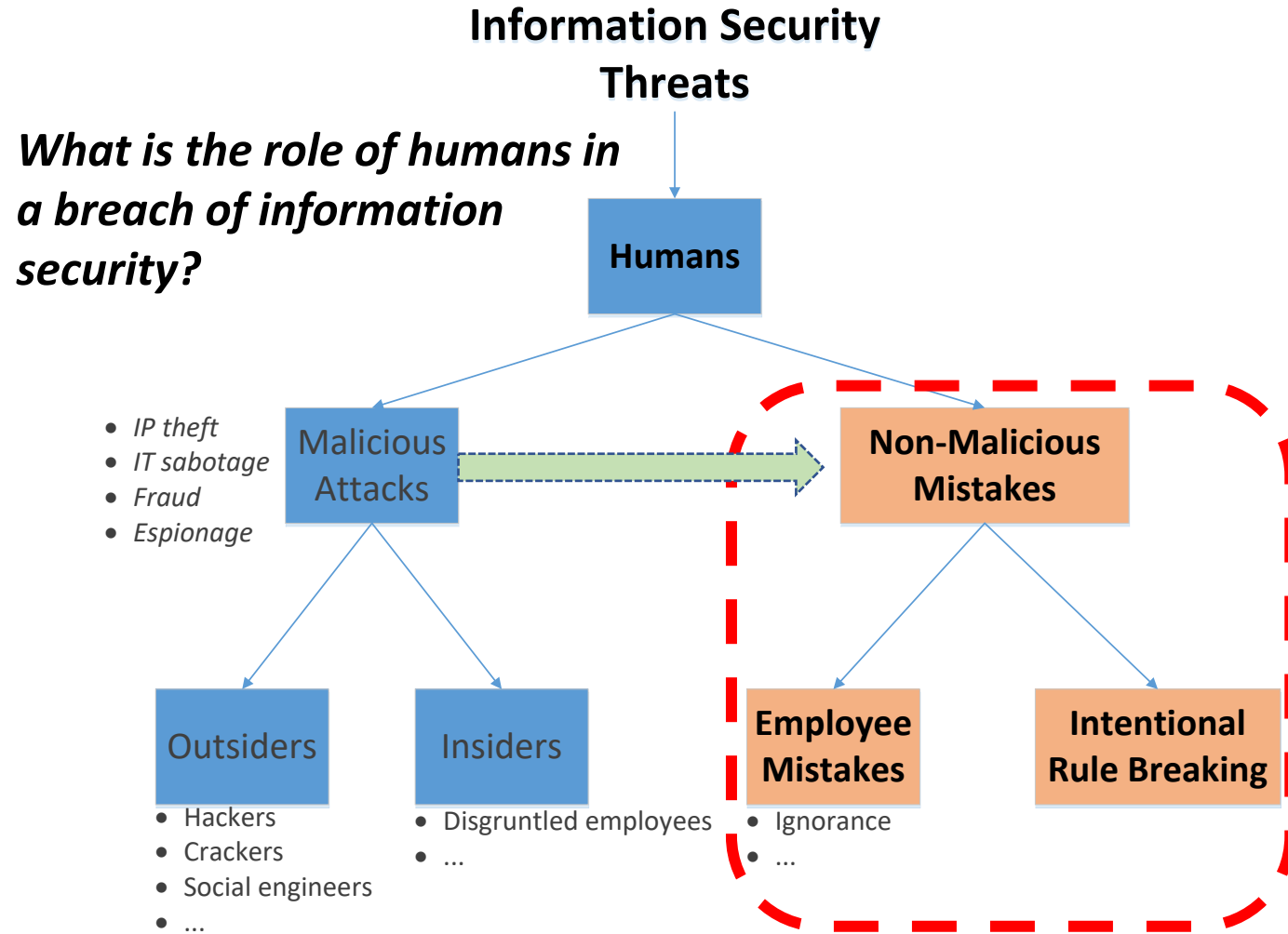


Figure 6. Threat actors in breaches over time

Verizon (2019) "Data Breach Investigations Report"

What roles do employees play in these attack chains

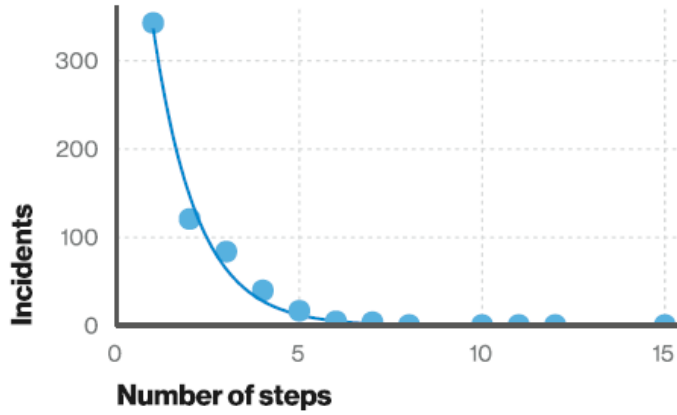


Figure 29. Number of steps per incident (n=1,285)
Short attack paths are much more common than long attack paths.

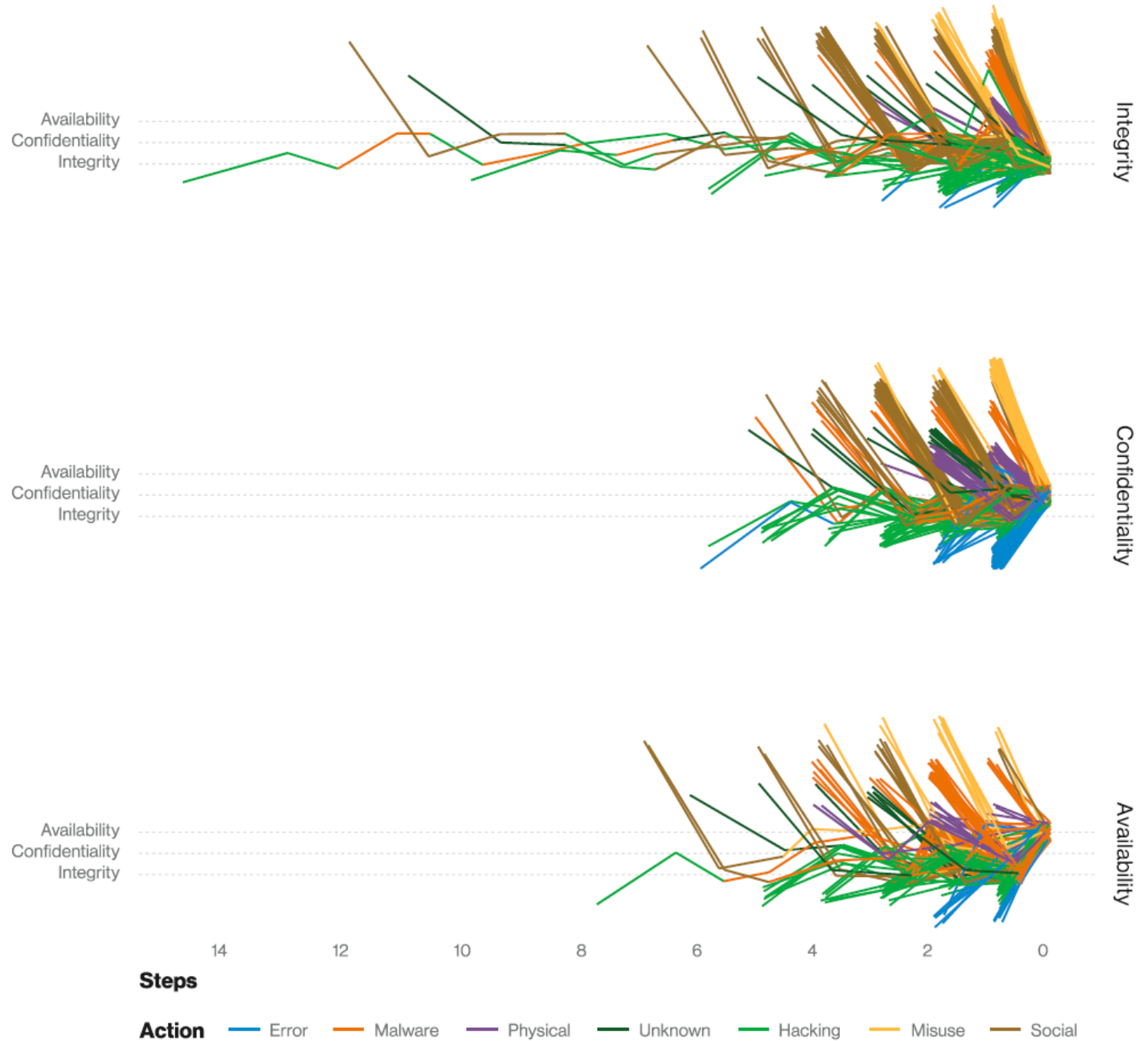





















































Figure 30. Attack chain by final attribute compromised¹² (n=941)

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware		1. Malware		
2. Web based attacks		2. Web based attacks		
3. Web application attacks		3. Web application attacks		
4. Denial of service		4. Phishing		
5. Botnets		5. Spam		
6. Phishing		6. Denial of service		
7. Spam		7. Ransomware		
8. Ransomware		8. Botnets		
9. Insider threat		9. Insider threat		
10. Physical manipulation/damage/theft/loss		10. Physical manipulation/damage/theft/loss		
11. Exploit kits		11. Data breaches		
12. Data breaches		12. Identity theft		
13. Identity theft		13. Information leakage		
14. Information leakage		14. Exploit kits		
15. Cyber espionage		15. Cyber espionage		

Legend: Trends:  Declining,  Stable,  Increasing
Ranking:  Going up,  Same,  Going down

In which of these threats are humans the vulnerability?

Employee Risk

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

Employee Risk

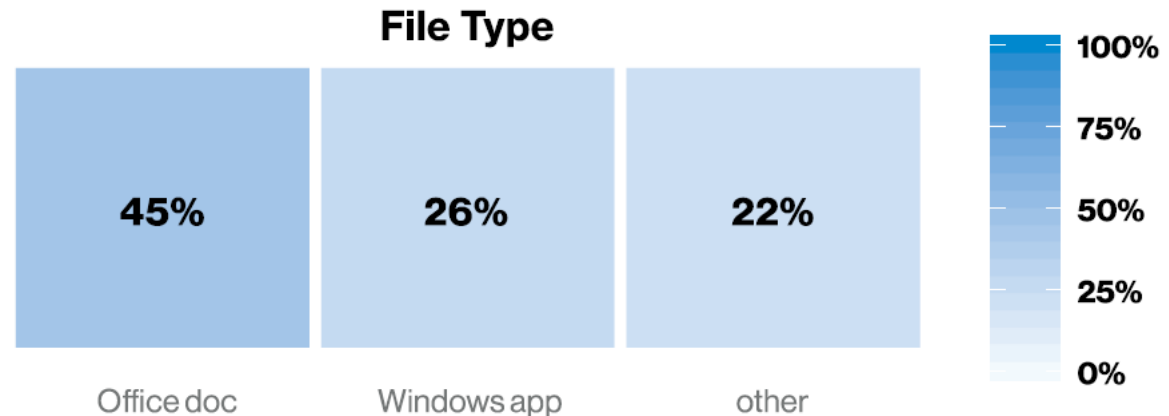
Verizon 2019 Data Breach Investigation Report

- 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



Why is teaching security awareness to employees 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...

Utah Medicaid contractor loses job over data breach

By Kirsten Stewart The Salt Lake Tribune

Published January 17, 2013 5:26 pm

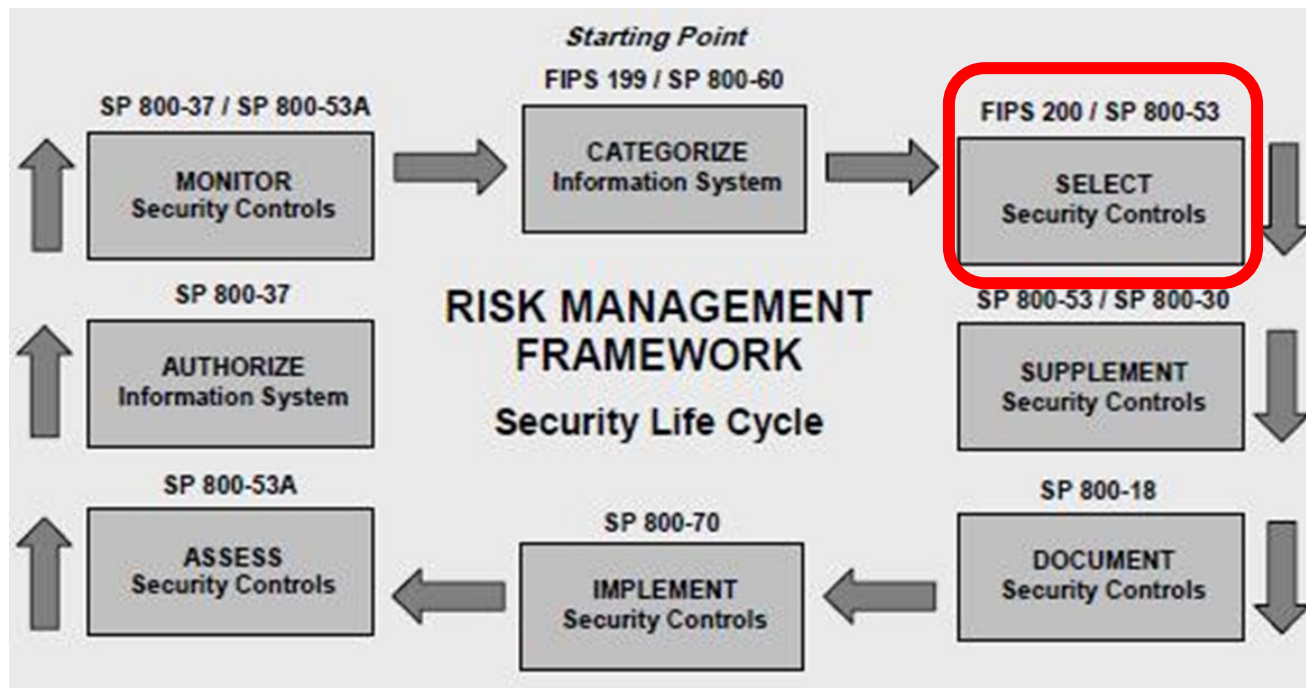
Health • Goold Health Systems CEO says mishap reinforces need to protect information.

“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...”

Agenda

- ✓ Human element of cyber security
- ✓ Employee risk
 - Cyber Security Employee Awareness and Training Risk Controls
 - Evolution of Organizations' Security Awareness and Training Programs
 - Training course content examples




NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>



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

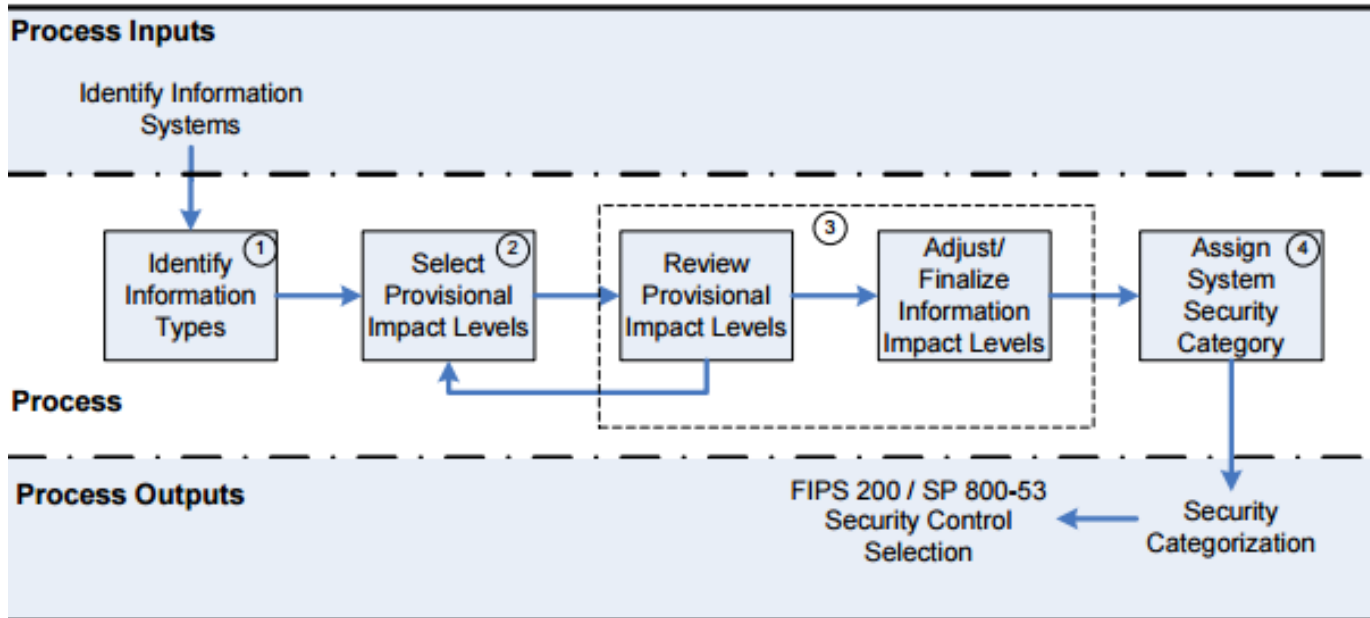
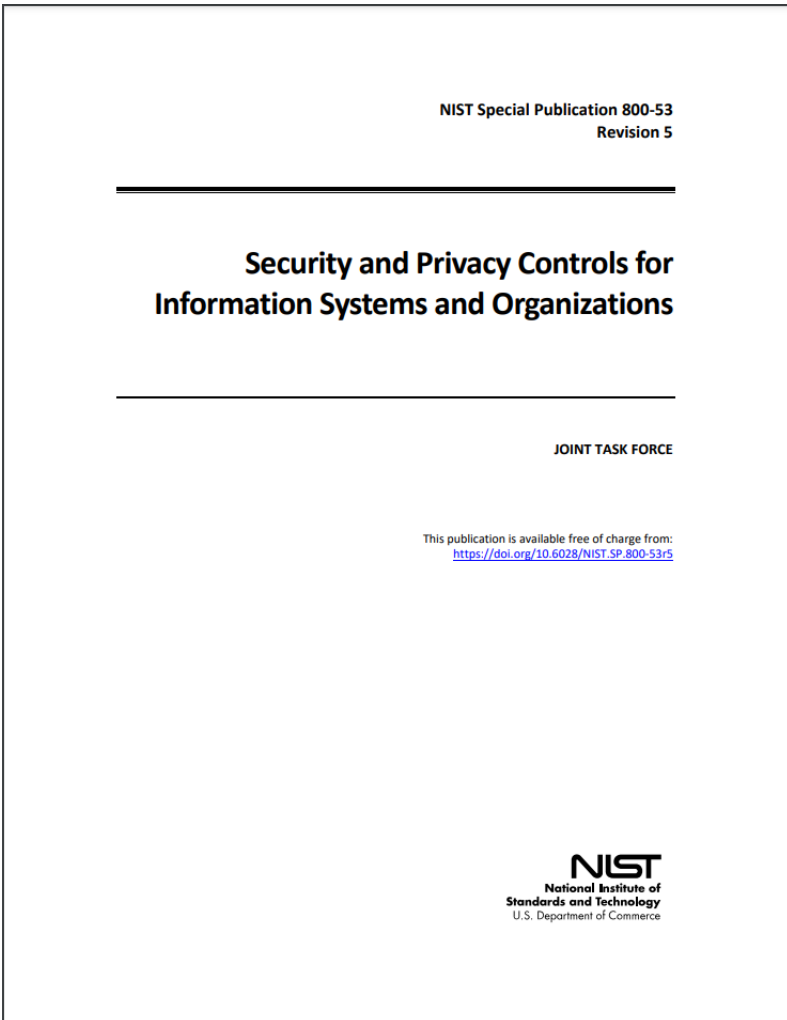


Figure 2: SP 800-60 Security Categorization Process Execution

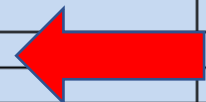
Guidelines for employee cyber security Awareness and Training risk controls




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

TABLE 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



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
	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


The guidelines for assessing cyber security risk controls

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.800-53A4>


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

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

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.800-53Ae4>


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

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

How do IT Auditors assess Security Awareness Training ?

Security Awareness Training control enhancement

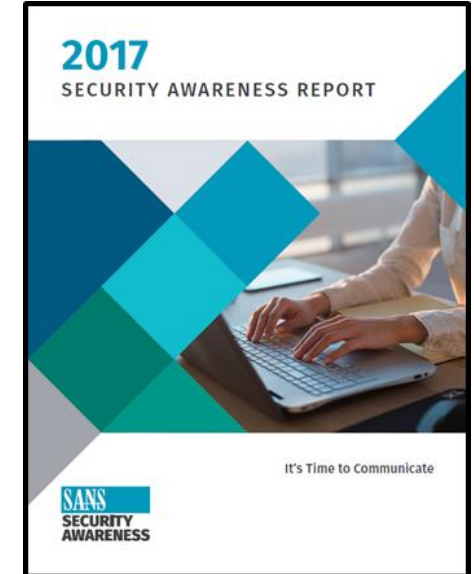
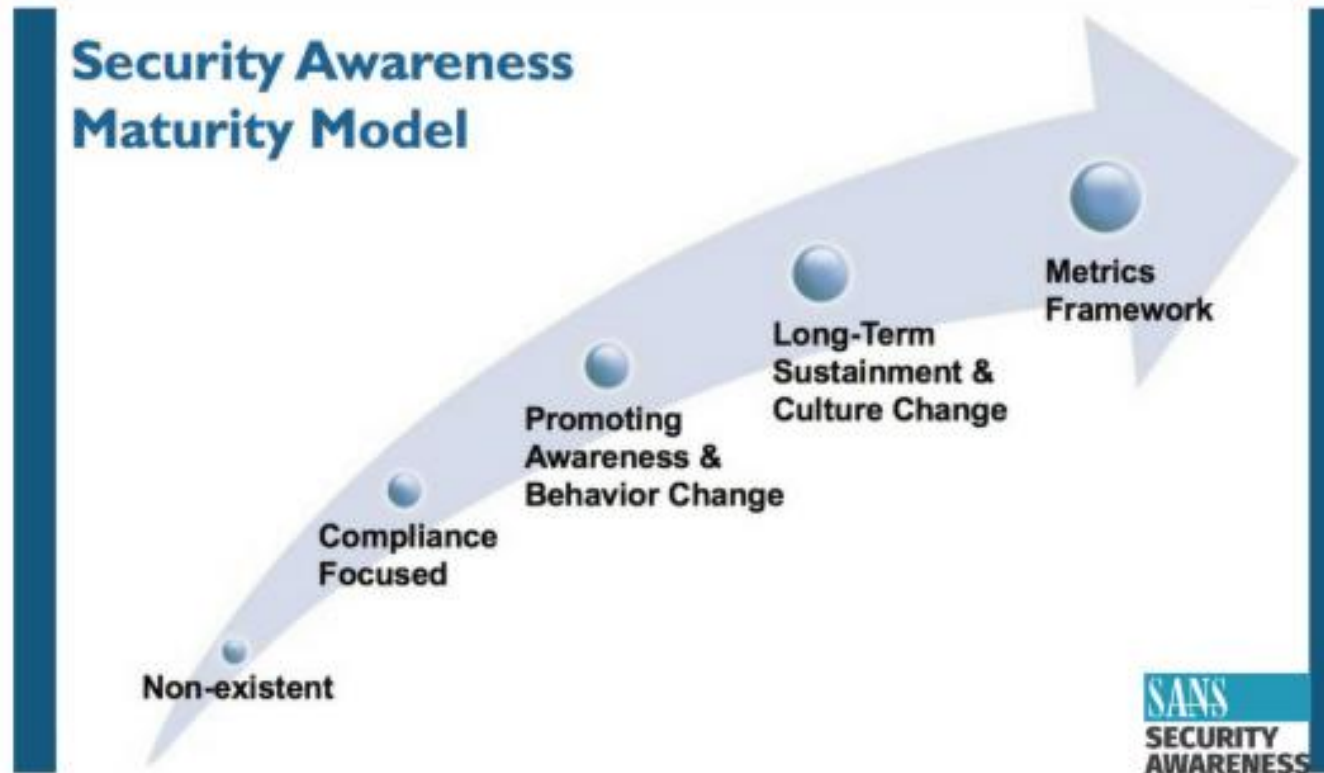
AT-2(2)	SECURITY AWARENESS TRAINING <i>INSIDER THREAT</i>
	<p>ASSESSMENT OBJECTIVE:</p> <p><i>Determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat.</i></p>
	<p>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</p> <p>Examine: [SELECT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

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

Agenda

- ✓ Human element of cyber security
- ✓ Employee risk
- ✓ Cyber Security Employee Awareness and Training Risk Controls
 - Evolution of Organizations' Security Awareness and Training Programs
 - Training course content examples

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



Maturity Level of Awareness Programs

How mature is the average security awareness program? Overall the numbers were very similar to last year, within 3 percentage points. It's heartening to see that more than half of respondents are currently promoting awareness and behavior changes, and are well on their way to establishing long term, sustainable programs.

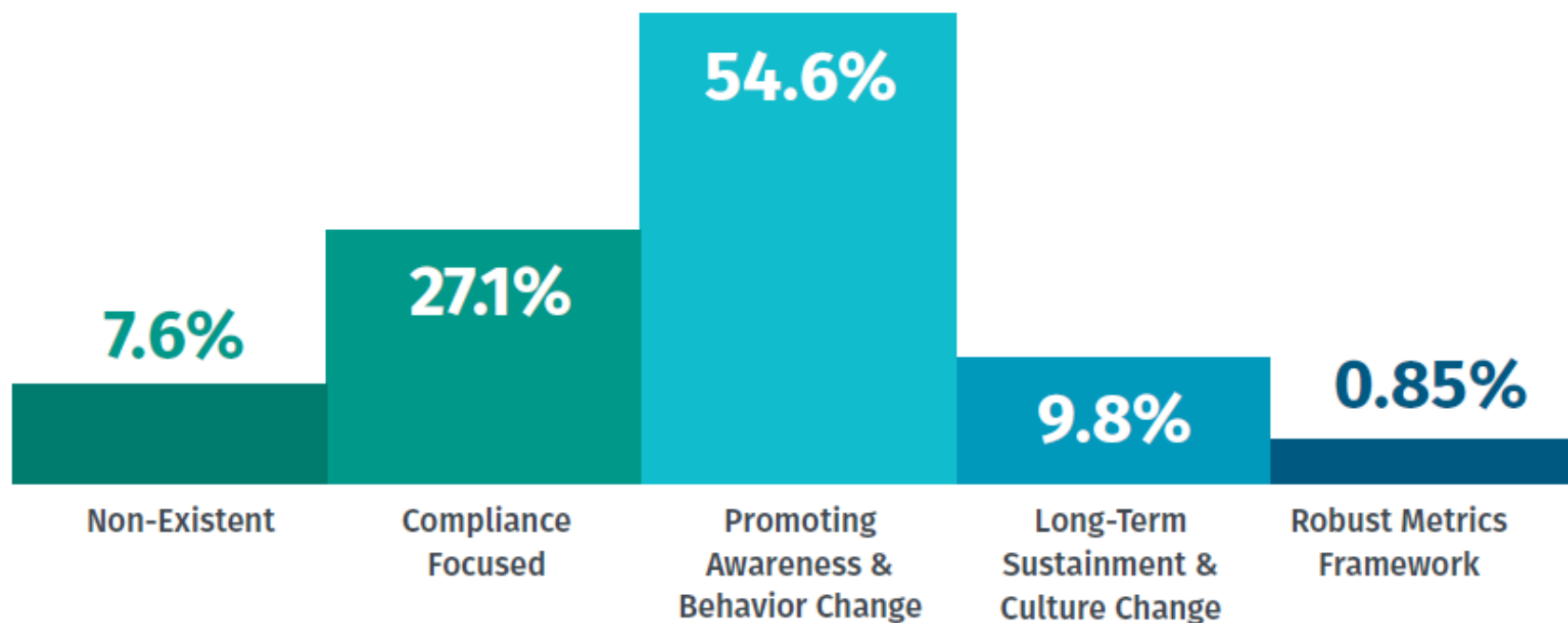


Fig. 2 - How mature is the average security awareness program?

Major Challenges	Responses	%
Communication	113	15.98%
Employee Engagement	101	14.29%
Time	95	13.44%
Culture	85	12.02%
Resources	83	11.74%
Upper Management Support	80	11.32%
Other	66	9.34%
Money	42	5.94%
Enforceability of Program	31	4.38%
Staff	11	1.56%
Total	707	100%

Fig. 4 - By the Numbers: Major Security Awareness Challenges

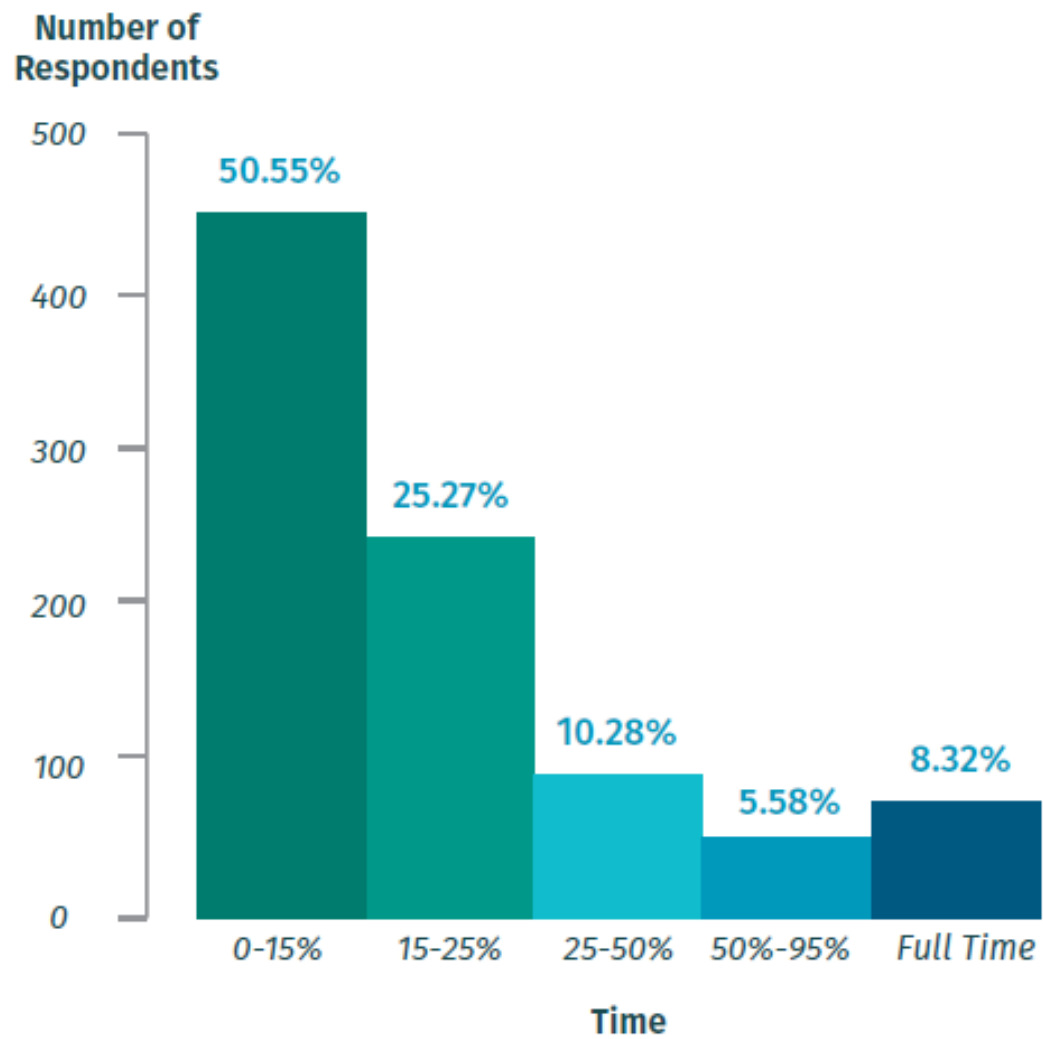


Fig. 7 - What percentage of your time is focused on security awareness?

Organization Size	Average Number of FTEs
1 - 500 People	1.28
500 - 1000 People	1.30
1000 - 5000 People	1.24
5000 - 25,000 People	1.58
25,000 - 100,000 People	2.09
100,000 People or More	2.45

Fig. 9 - Average Number of Security Awareness FTEs per Organization Size

**This graph doesn't represent what we recommend for the number of FTEs dedicated to awareness. Instead, it shows the average number of FTEs organizations currently have. Refer to Figure 8 for FTE recommendations.*

How many people do you need in an organization to promote information security awareness and provide training?

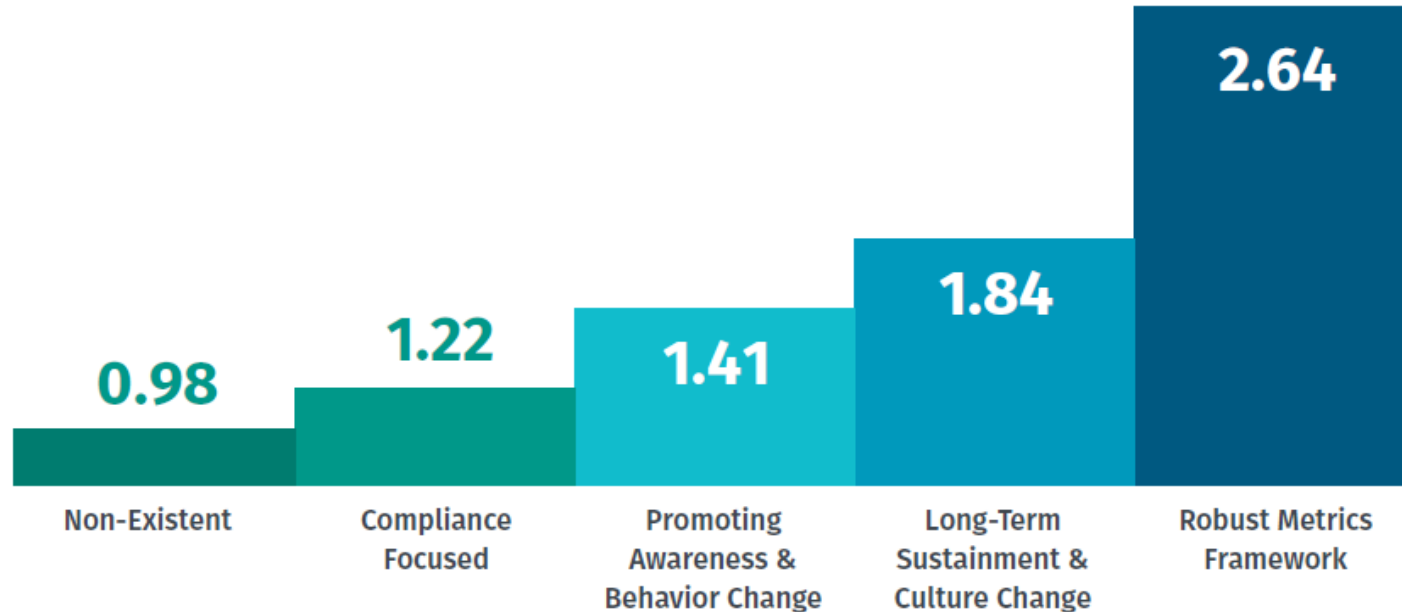


Fig. 8 - Average Number of FTEs by Maturity Level*

**This shows the minimum number of FTEs you need dedicated to awareness to achieve each maturity level. Organizations larger than 5,000 people most likely need more FTEs. Assumptions made as follows: 4+ answers were counted as 4, less than one response was counted as 0.5*

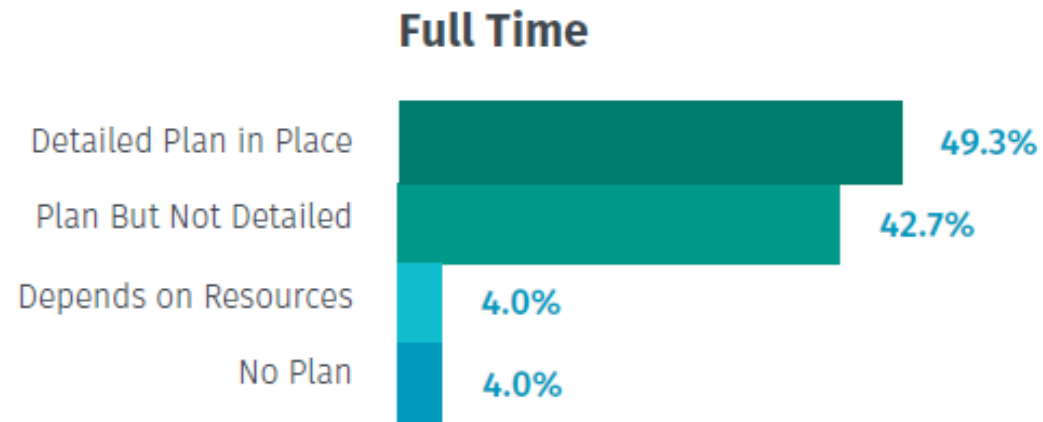
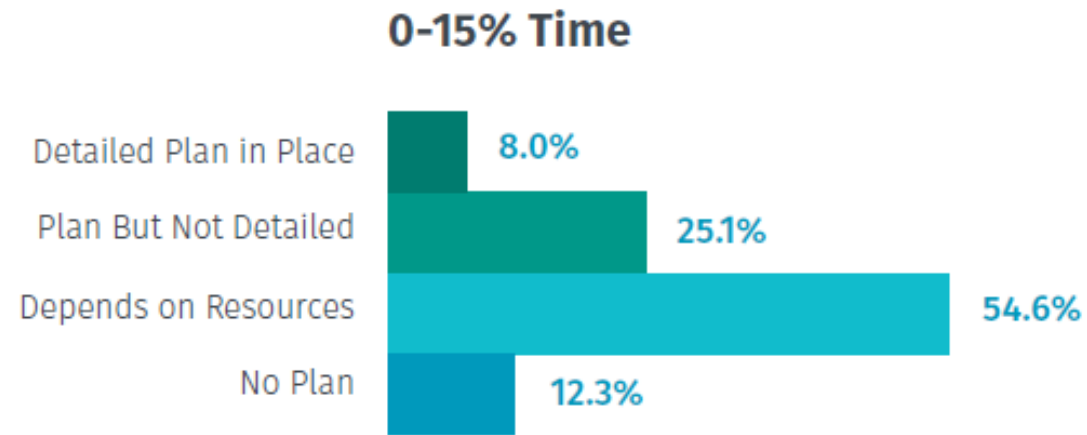


Fig. 10 - Time Spent on Security Awareness Planning

Recapping on the importance of time, we've outlined that to have a thriving program you need:

- 1. FTEs:** You need at least 1.4 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 2.6 FTEs.
- 2. Partnerships:** Build partnerships and collaborate with others in your organization to help you.
- 3. Buy Time:** If you have budget, use that to buy yourself time. Hire people to help you get your awareness program off and running.
- 4. Ambassadors:** For awareness programs that are more mature, consider building a security ambassador program. This is when you build a network of volunteers throughout your organization to help engage fellow employees and push your message out.

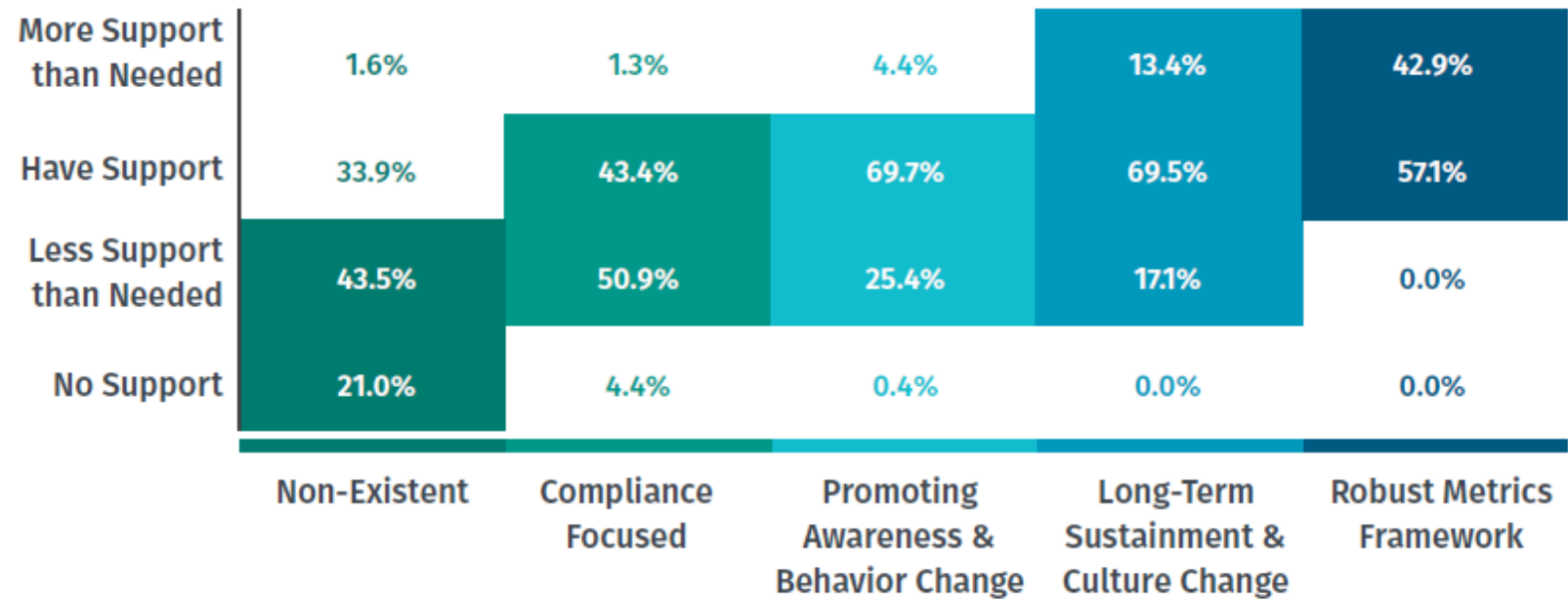


Fig. 14 - Leadership Support by Security Awareness Maturity Level

Communication is highly-valued in starting, growing, and expanding a security awareness program.

- 1. Leadership:** Dedicate a certain amount of time each month for communicating to leadership about your security awareness program. Make sure you communicate to leaders every month in the vernacular that business leaders will value.
- 2. Champion:** Find yourself a strong champion within leadership. Use that leader either to help communicate the value of your program to other leaders, or have them help you craft your message in the language that is actionable to other leadership.
- 3. Partnership:** Don't have the skills you need to effectively communicate? Then partner with those that do.
- 4. Communications Training:** Learn the skills you need to effectively communicate. Just because you may not have the skills today, doesn't mean you won't have them next year.
- 5. Human Resources:** Work with human resources to better understand your organizational culture and connect with new hires.
- 6. Target Audiences:** As your awareness program matures, begin to identify different target groups in your organization. Organize your communications plan based on what resonates best for each target group (such as IT admins, developers, field engineers, faculty, doctors, etc.).

Conclusion

Ultimately, security awareness is hard. However, there are some key steps you can take to improve your program. Whether you're able to dedicate your time fully to the improvement and success of your awareness program or if you only have a small part of each week to focus on it – there are two major takeaways identified as critical to a thriving program. Time and Communication. Without these two important pieces, it'll be difficult to get legs to your program and successfully protect your organization and the people within it.

Agenda

- ✓ Human element of cyber security
- ✓ Employee risk
- ✓ Cyber Security Employee Awareness and Training Risk Controls
- ✓ Evolution of Organizations' Security Awareness and Training Programs
- Training course content examples

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.

Training course content example

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

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

Training course content example

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

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

Training course content

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

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



Agenda

- ✓ Human element of cyber security
- ✓ Employee risk
- ✓ Cyber Security Employee Awareness and Training Risk Controls
- ✓ Evolution of Organizations' Security Awareness and Training Programs
- ✓ Training course content examples