

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: CXO-T09

Understand and Manage Your Human Risk

Lance Spitzner

Director, SANS Security Awareness

lsplitzner@sans.org

[@lsplitzner](https://twitter.com/lsplitzner)




#RSAC

The Problem

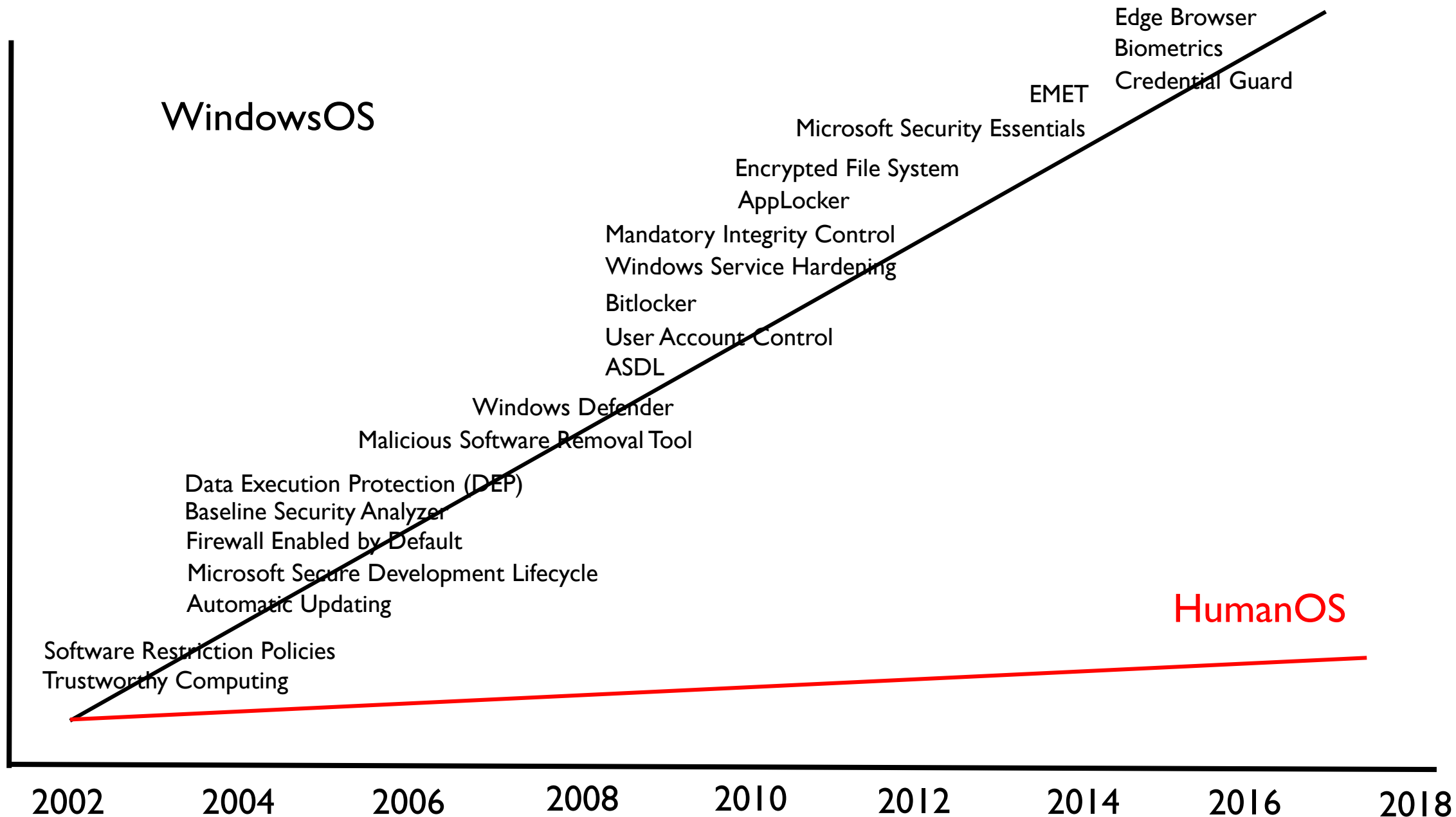
cyber attack

ng the industries
sharp increase in

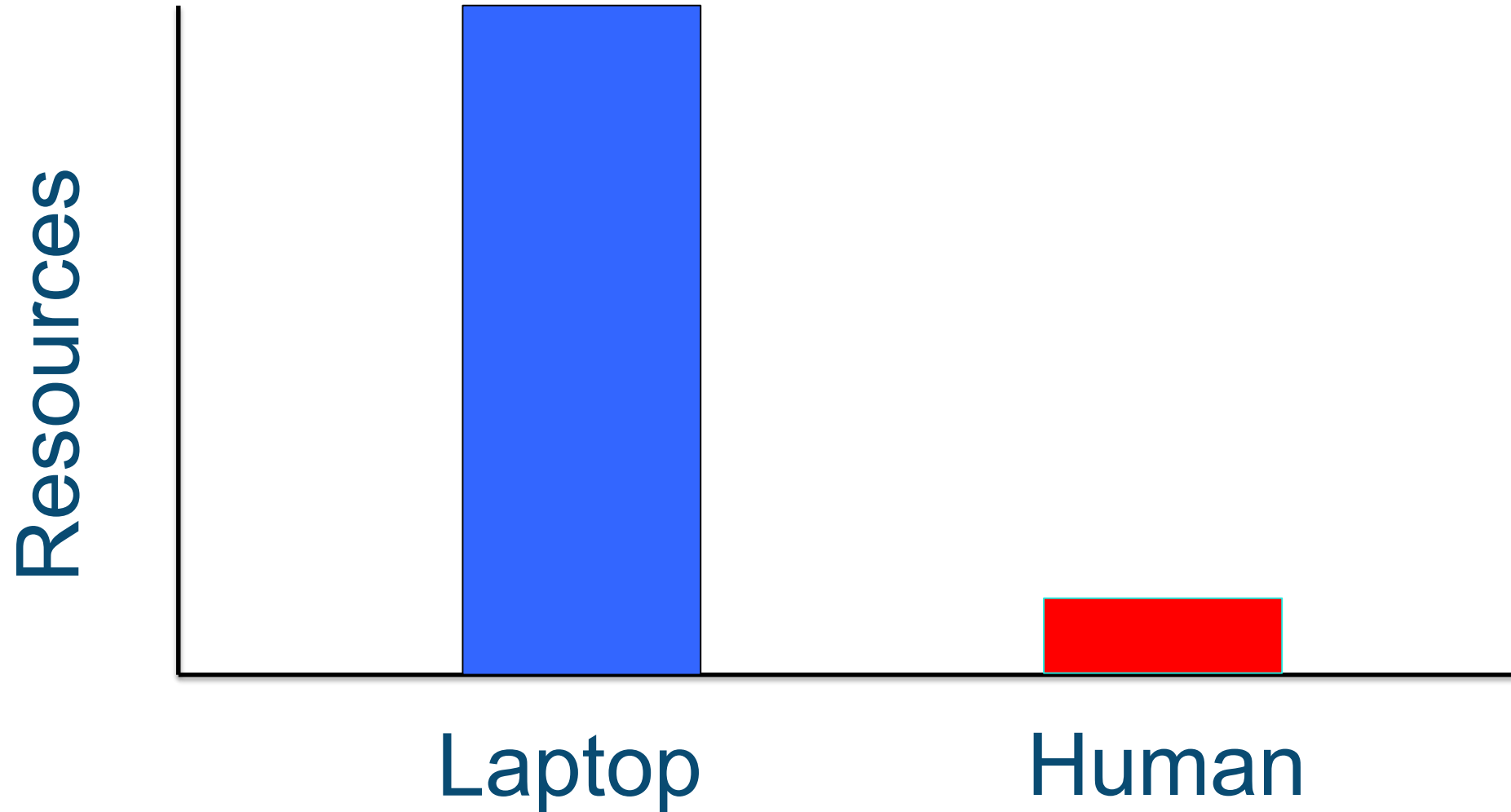


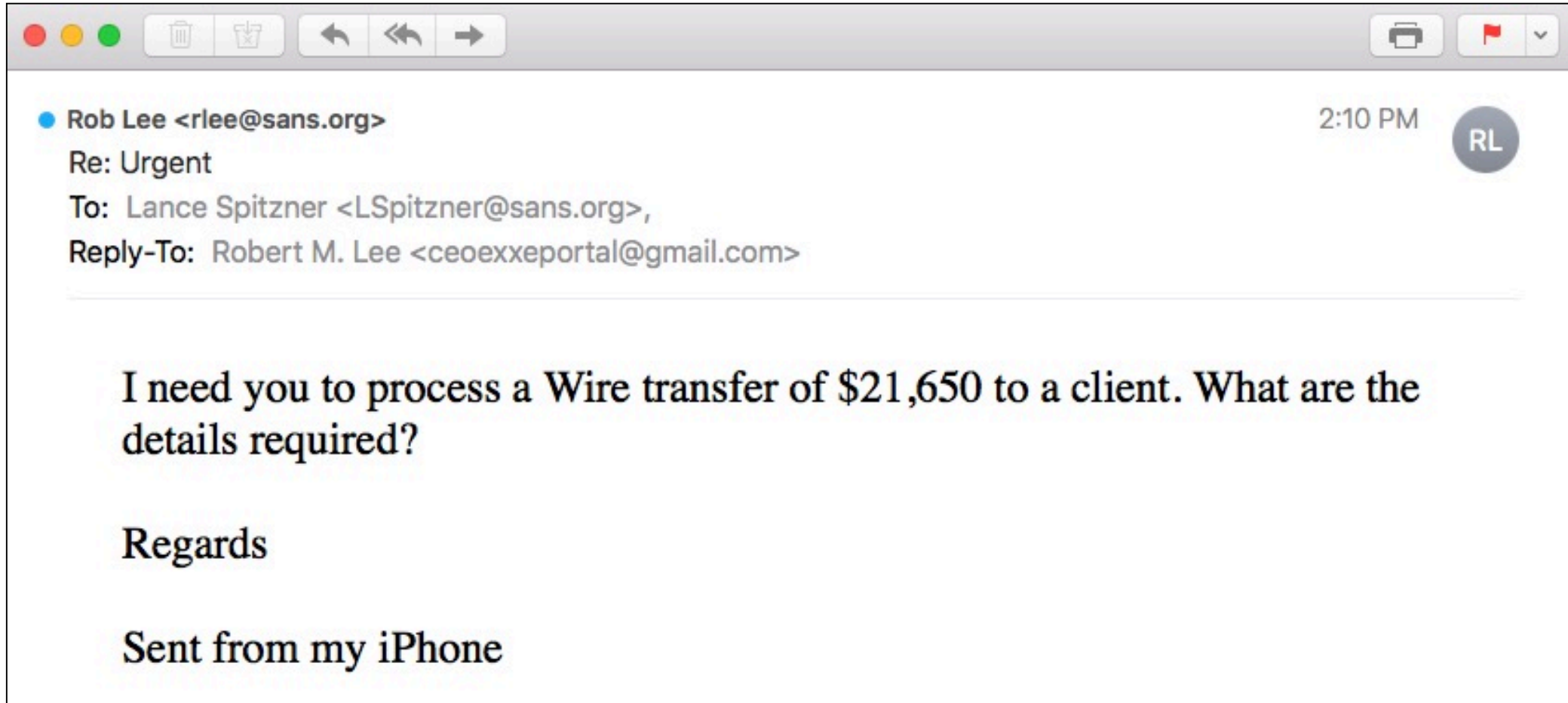
*People are not the weakest link,
they are the primary attack
vector.*

Security Controls



Technology vs. Human Investment





● Rob Lee <rlee@sans.org>

2:10 PM

RL

Re: Urgent

To: Lance Spitzner <LSpitzner@sans.org>,

Reply-To: Robert M. Lee <ceoexxeportal@gmail.com>

I need you to process a Wire transfer of \$21,650 to a client. What are the details required?

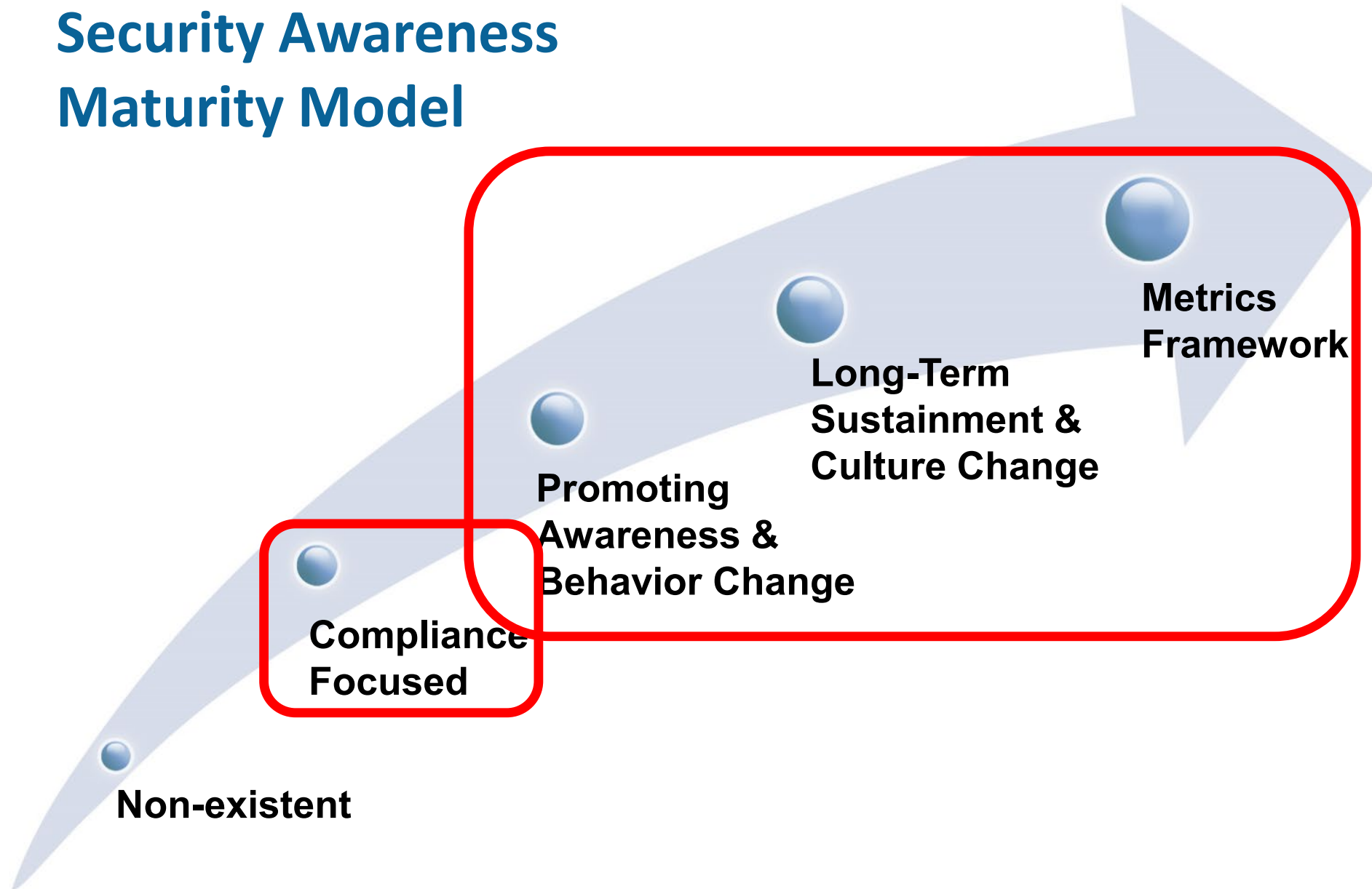
Regards

Sent from my iPhone

The Solution

A woman in a dark sleeveless top and glasses stands in front of a large whiteboard, gesturing with her right hand. She is addressing a group of people seated at desks in a modern office with a brick wall background. The audience includes a man in a light blue shirt and glasses, and another man in a dark suit. The scene is brightly lit, with large windows visible on the right side of the frame.

Security Awareness Maturity Model



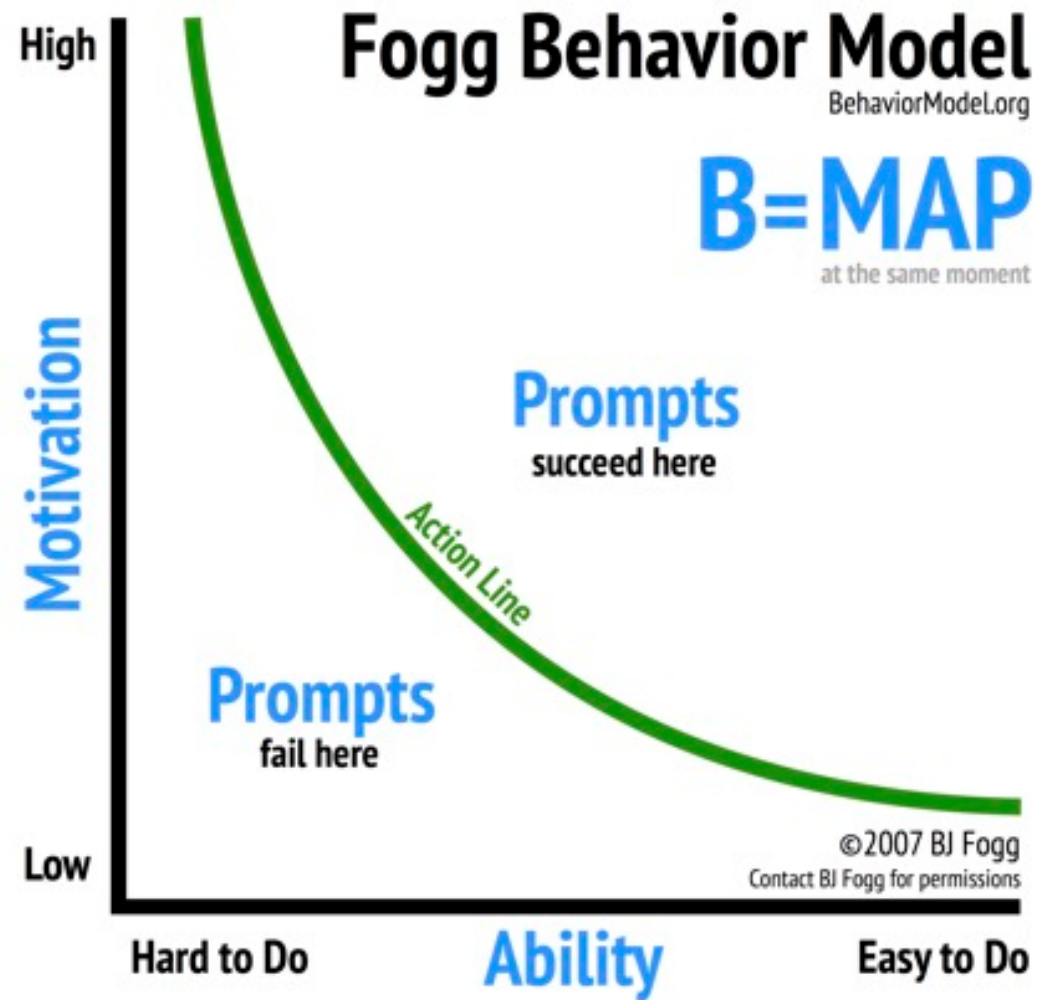
Common Misconceptions / Blockers

Awareness
programs never
work

Awareness
programs are a
failure because
someone always
clicks

Awareness is just
about human
prevention

VULNERABILITIES x THREATS x IMPACT



Start With a Strategy

- What is the overall goal of the program?
- What objectives support that goal?
- What is the scope?
- What key metrics measure success?

Goal

Ensure compliance with required regulations and standards, and to identify and manage our human risk to an acceptable level.

Objectives

- Ensure compliance with GDPR, PCI DSS and GLBA.
- Identify and manage our top five human risks.
- Reduce attacker dwell time by 40% through creation of Human Sensor network.
- Create a positive, cyber-aware culture where people feel responsible for and value cyber security.

Three Key Elements to a Strategic Plan

Who?

Who you are
targeting in your
program?

What?

What behaviors do
you want them to
change or exhibit?

How?

How will you
change those
behaviors?

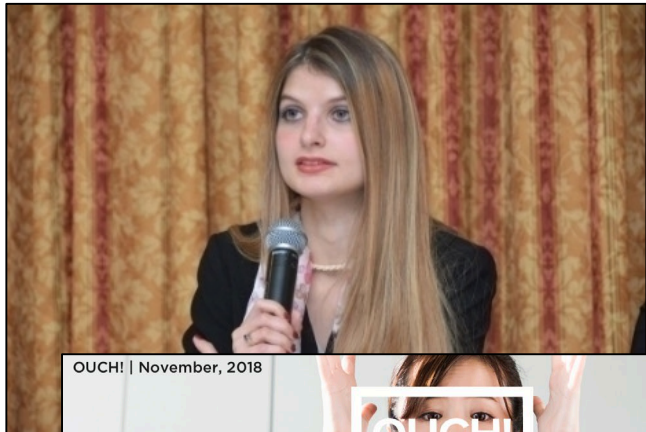
Top Risk Groups

- New programs often start with everyone.
- As your program matures, identify high risk groups
 - Developers
 - Leadership
 - Accounts Payable / Financial Transactions
 - Human Resources
 - Help Desk
 - Interns

Manage Your Top Human Risks

- Social Engineering / Phishing
- Passwords
- Accidental

Once you identify your top human risks, what are the key behaviors that manage those risks?



OUCH! | November, 2018

SANS
SECURITY
AWARENESS

OUCH!








The Monthly Security Awareness Newsletter for You

Am I Hacked?

Overview

Just like driving a car, sooner or later you may have an accident no matter how secure you are. Below are clues to help figure out if you have been hacked and, if so, what to do. The sooner you identify something bad has happened, the more likely you can fix the problem.

Clues You Have Been Hacked

-  Your anti-virus program generates an alert that your system is infected. Make sure it is your anti-virus software generating the alert, and not a pop-up window from a website trying to fool you into calling a number or installing something else. Not sure? Open your anti-virus program.
-  You get a pop-up window saying your computer has been encrypted and you have to pay a ransom to get your files back.
-  Your browser is taking you to all sorts of websites that you did not want to go to.
-  Your computer or applications are constantly crashing or there are icons for unknown apps or strange windows popping up.
-  Your password no longer works even though you know it is correct.
-  Friends ask you why you are spamming them with emails that you know you never sent.
-  There are charges to your credit card or withdrawals from your bank account you never made.

How to Respond

If you suspect you have been hacked, the sooner you act the better. If the hack is work related, do not try to fix the problem yourself; instead, report it immediately. If it is a personal system or account that has been hacked, here are some steps you can take:

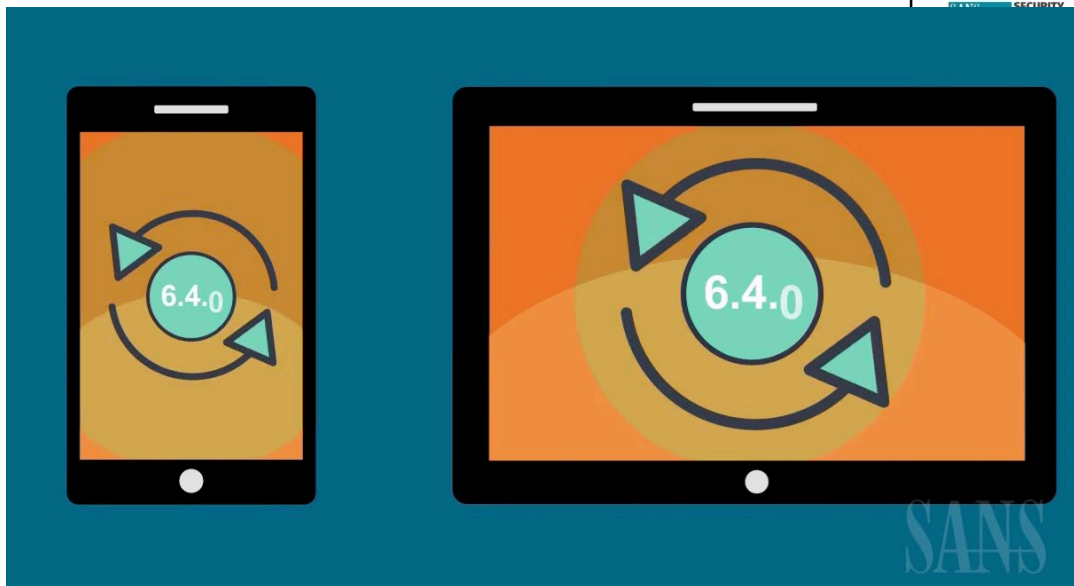
Whoops... You just got phished!

Fortunately this was an **authorized training simulation**, but if it had been a real phishing attempt, your online safety could have been compromised. Opening and reading email is fine, but clicking on malicious links or attachments could cause you harm.



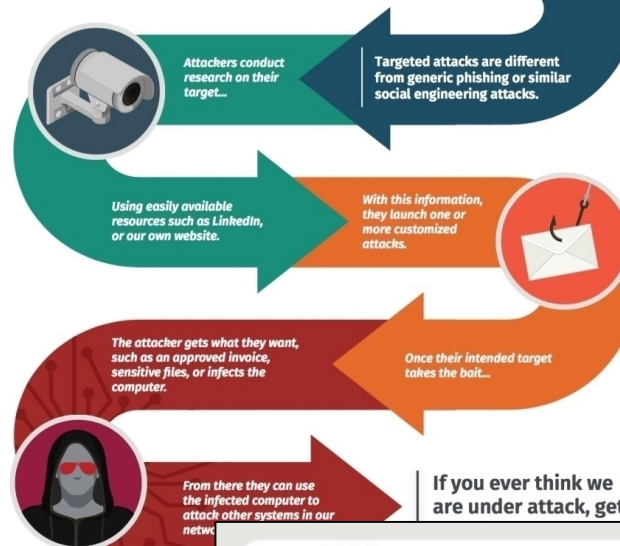
Common clues of a phishing attack

- Messages that create a tremendous sense of urgency may be trying to rush you into making a mistake.
- If it sounds too good to be true, it probably is (no, you did not just win the lottery).
- Official organizations don't usually send messages that are full of grammatical errors and spelling mistakes. They also don't come from personal email addresses (such as @gmail.com, @yahoo.com, or @hotmail.com).
- Messages that open with "Dear Customer" or some other generic greeting should get close scrutiny.
- No legitimate organization should request highly sensitive information over email such as your credit card number or account password.
- The message comes from someone you know, but they just don't sound quite right. Cyber attackers can send emails that look like they come from your boss, co-worker, or friend in order to gain your trust.



What You Need to Know About

Targeted Attacks



Metrics

What metrics can you use to measure and communicate impact?

- Compliance metrics
- Behavior metrics
- Strategic metrics

Metric Name	What Is Measured?	How Is it Measured?	When Is it Measured?	Who Measures?	Details	
Training Completion	Who has or has not completed annual security awareness training	Reports from LMS or sign-in sheets for onsite workshops	Annually	Who ever is responsible for primary training	Primary training is when people are taught all awareness material for the first time or in a single sitting, usually online computer-based training (CBT) or onsite workshops.	
					For a security awareness program to have an impact, it must be communicated to people on a regular basis. This metric measures other communication methods and training modalities that repeat and reinforce key learning objectives from the primary training.	
Communication Methods	Metric Name	What Is Measured?	How Is it Measured?	When Is it Measured?	Who Measures?	Details
	Phishing Awareness	Number of people who fall victim to a phishing simulation. The definition of falling victim is clicking on the link or opening an attachment.	Phishing assessment	Monthly	Security team	These attacks replicate the very same ones cyber attackers are using. The goal is to measure who falls victim to such attacks. This number should decrease over time as behaviors change.
	Phishing Reporting	Number of people who detect and report a phishing email (regardless if its an assessment or real attack)	Phishing assessment	Monthly	Security team	Uses the above methodology, but instead of tracking who falls victim, it tracks who identifies the attacks and reports them. This number should increase over time. This is developing the Human Sensor
	Phishing Repeat Offenders	Number of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behavior and represent a high risk.	Phishing assessment	Monthly	Security awareness team	These individuals represent a high risk to an organization and must be addressed. This can include in escalation in training and consequences, moved to a different job role or department, or managed in some other way.
Policy Sign-off	Facility Physical Security	Number of employees who understand, follow, and enforce your policies for restricted or protected access to facilities.	Test how many employees are wearing their badges or stopping those who are not.	Monthly or weekly	Information security or physical security	For many organizations, physical security is a major control in reducing risk, especially when dealing with secured facilities. This metric will test and measure people's understanding and enforcement of this control.
		When employees connect to an				

website fact sheets

podcasts

social media channels (such as Yammer or Slack)

Employees may be required to document that employees not only understand and will follow the training.

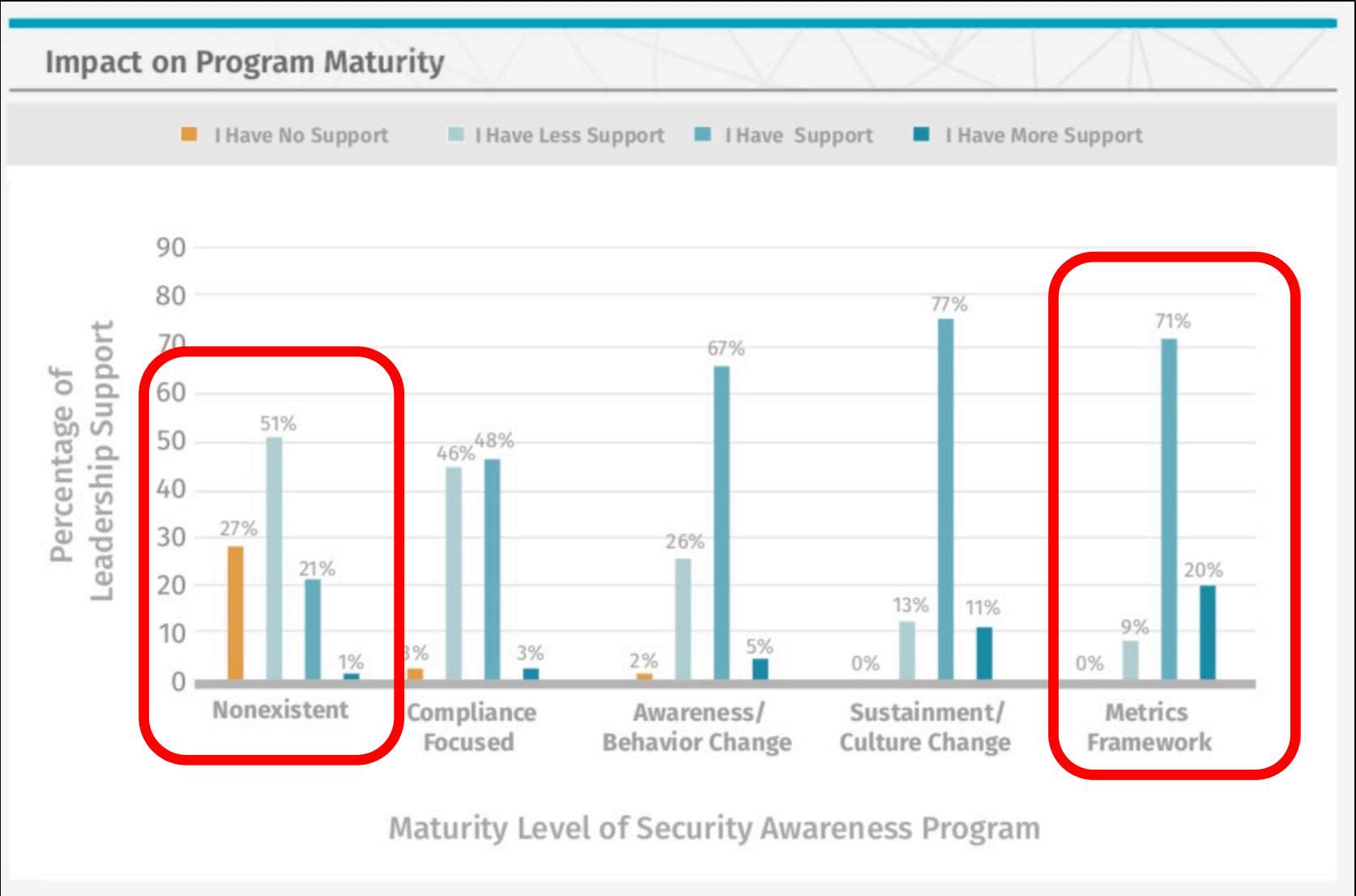
Metric Name	What Is Measured?	How Is it Measured?	When Is it Measured?	Who Measures?	Details
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walkthrough	Monthly or weekly	Information security	
Passwords	Number of employees using strong passwords.	Password brute forcing	Monthly or quarterly	Security	Time to Detect an Incident What is the average time it takes to detect an incident? Standard incident report tracking processes Monthly Incident Response Team or Security Operations Center The time to detect an incident should decrease as the Human Sensor is developed. This is a critical metric as it is key to creating a resilient organization.
Social Engineering	Number of employees who can identify, stop, and report a social engineering attack.	Phone call assessments	Monthly	Security	Policy Violations Number of times workforce violates organizational security policies. Standard violation reporting processes Monthly Human Resources or security team As the workforce better understands organization policies, or as those policies become easier to follow, workforce is more likely to follow them.
Sensitive Data	Number of employees posting sensitive organizational information on social networking sites.	Online searches for key terms	Monthly	Security	Data Loss Incidents Number of times there is a data loss incident, either accidental or due to a deliberate attack. Standard incident report tracking processes Monthly Security or Data Loss Prevention team As your workforce better understand the policies and behaviors they are supposed to follow, the number of data loss incidents should fall.
Data Wiping or Destruction	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.	Random	Information security	Infected Computers Number of infected computers. Help Desk or centralized AV management software Monthly Help Desk or Security Operations Center Most infected computers are a result of human behavior (infected attachments, malicious links, etc.). This number should go down over time as employees are trained.
Device Physical Security	Number of employees who left their devices unsecured in their cars in the organization's parking lot.	Do a physical walkthrough of the parking lot and identify any cars that have devices that are visible on a car seat.	Monthly	Information security	Privileged Account Abuse Number of privileged users that improperly use or abuse their privileged access Standard violation reporting processes Monthly Security team As your technical workforce better understand the policies and behaviors they are supposed to follow, the number of privileged access violations should fall.
Engagement	Number of requests the security awareness team gets to do security briefings for other business units or teams	Tracking by the security awareness team.	Monthly	Security team	Misconfigured Systems Number of incidents of systems or applications misconfigured Standard violation or incident reporting processes Monthly Incident Response Team or Security Operations Centers As your technical workforce better understand the policies and behaviors they are supposed to follow, the number of privileged access violations should fall.
Knowledge	Does workforce know and understand what is expected of them?	Knowledge assessments and online quizzes	Annual or after training	Leadership or Security Awareness team	Compliance or Audit Violations Number of compliance or audit violations or fines. Audit or compliance reports Annual Audit, Compliance or Governance teams One of the goals of security awareness is to help meet the requirements of certain standards or regulations.
Workforce attitudes towards security	Does the workforce understand the need for security, the important role they play, and support the behaviors needed?	Cultural survey	Annual or after training	Leadership or Security Awareness team	To measure your security culture you need to understand peoples attitudes, beliefs and perceptions of cybersecurity and the role it plays.

Three “S”s to Success

- Support
- Staff
- Soft skills



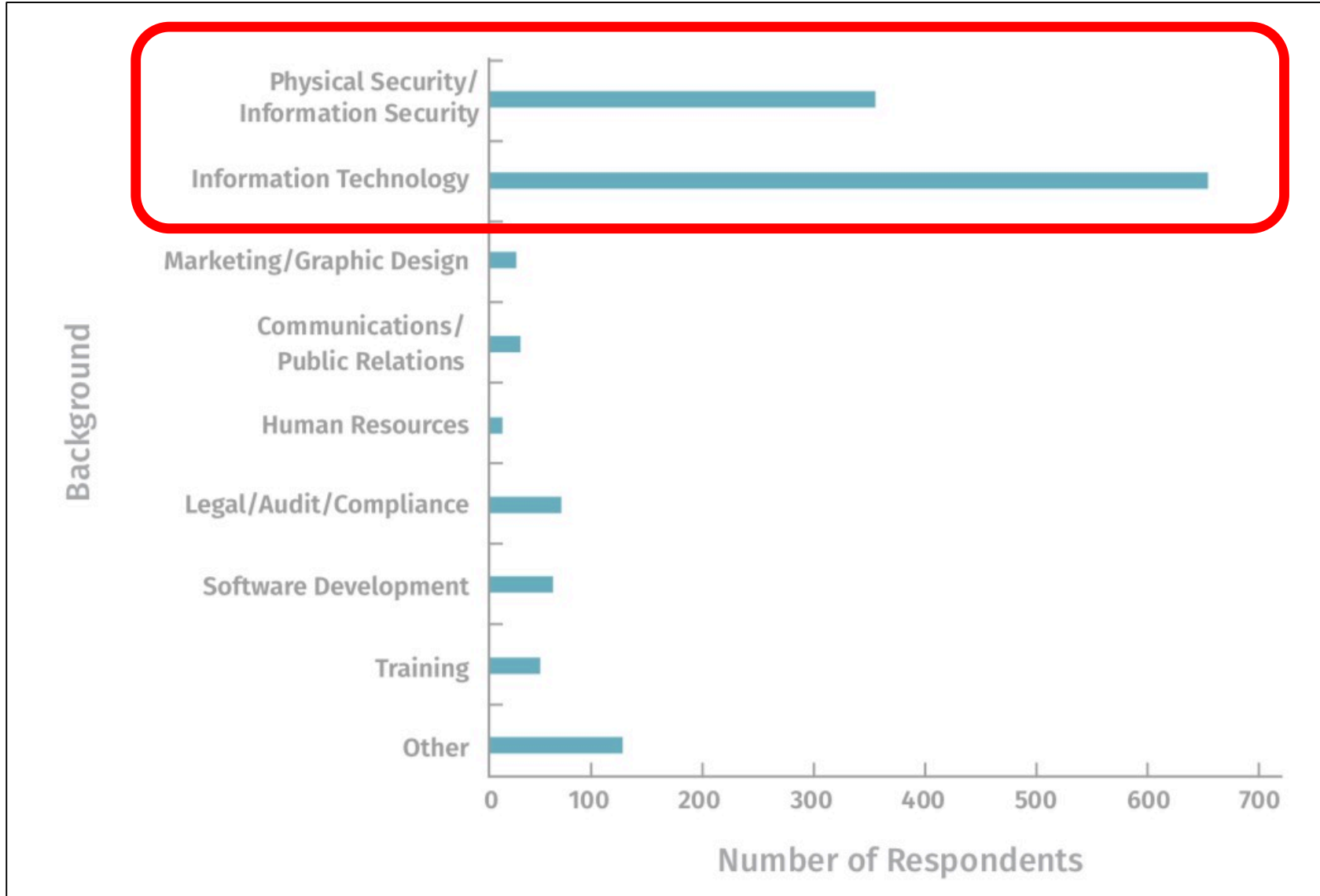
Leadership Support is Key



Minimum Number of FTEs

Average Number of FTE's Per Maturity Level	
Maturity Stage	Average FTE
Nonexistent	0.81
Compliance Focused	1.60
Awareness/Behavior Change	1.93
Sustainment/Culture Change	2.70
Metrics Framework	3.67

Soft Skills Lacking



When You Go Back - Ask

- Who is in charge of our awareness program?
- How many people are dedicated to our program?
- Where is our communication expertise?
- Who / What are our top human risks, how do we know?
- What is our overall strategy for engagement?
- How do we measure success?

Summary

- Until we also start addressing the human element, bad guys will continue to win.
- To manage human risk we need to change behavior. To change behavior we need a mature awareness program using a proven framework.

RSAConference2019

lspitzner@sans.org

An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, light blue lines that form overlapping circles and arcs. Small blue dots are scattered along these lines, creating a network-like or orbital pattern. The overall effect is a sense of dynamic movement and interconnectedness.