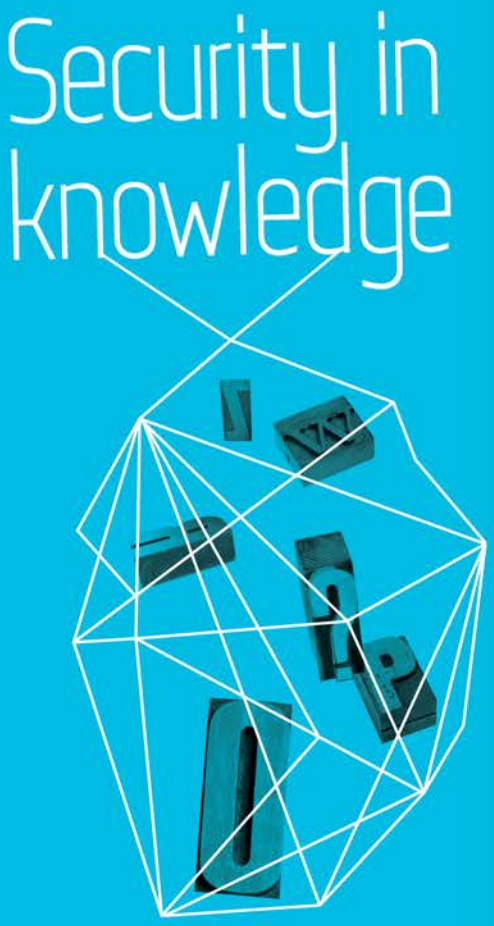
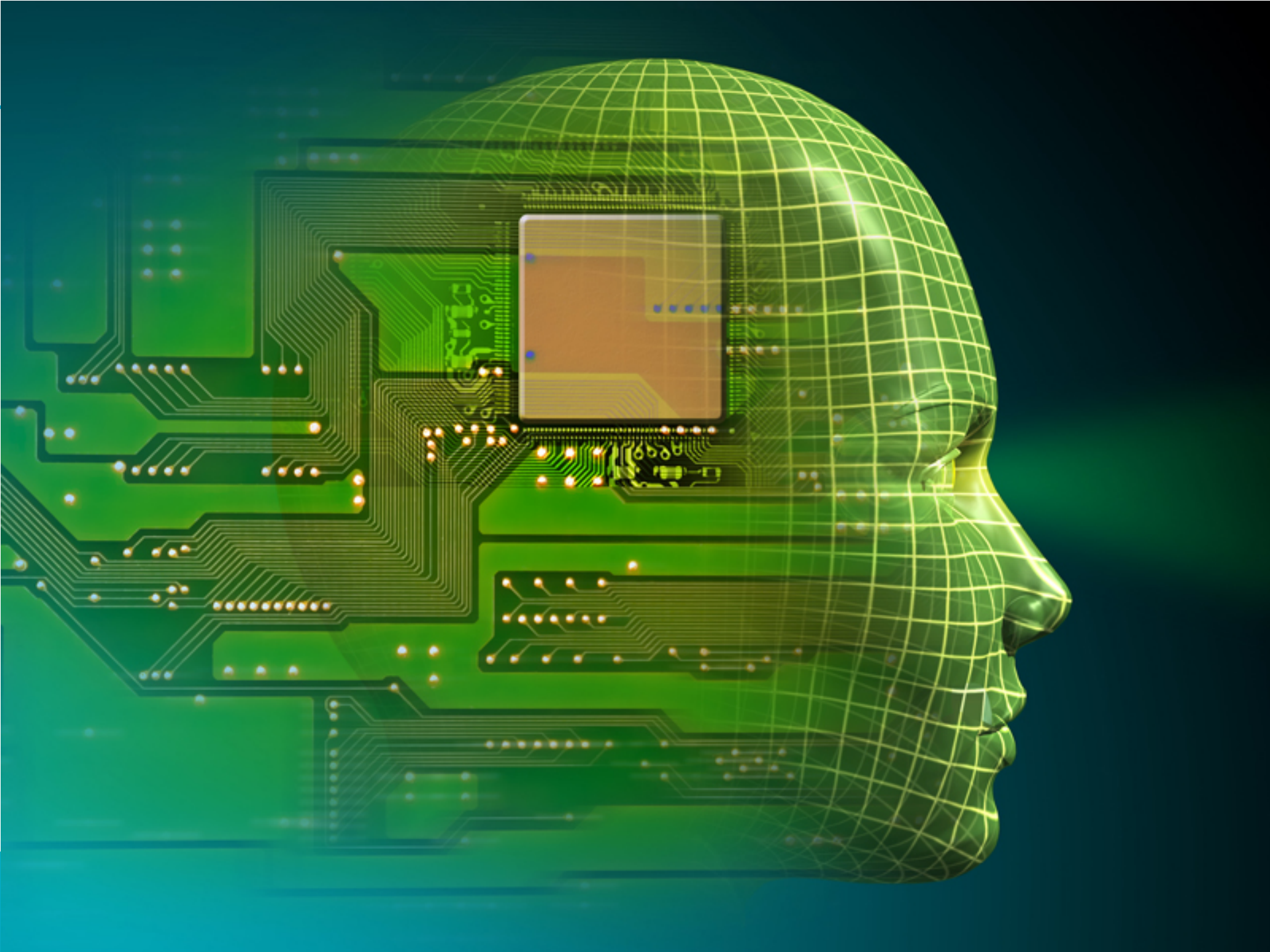
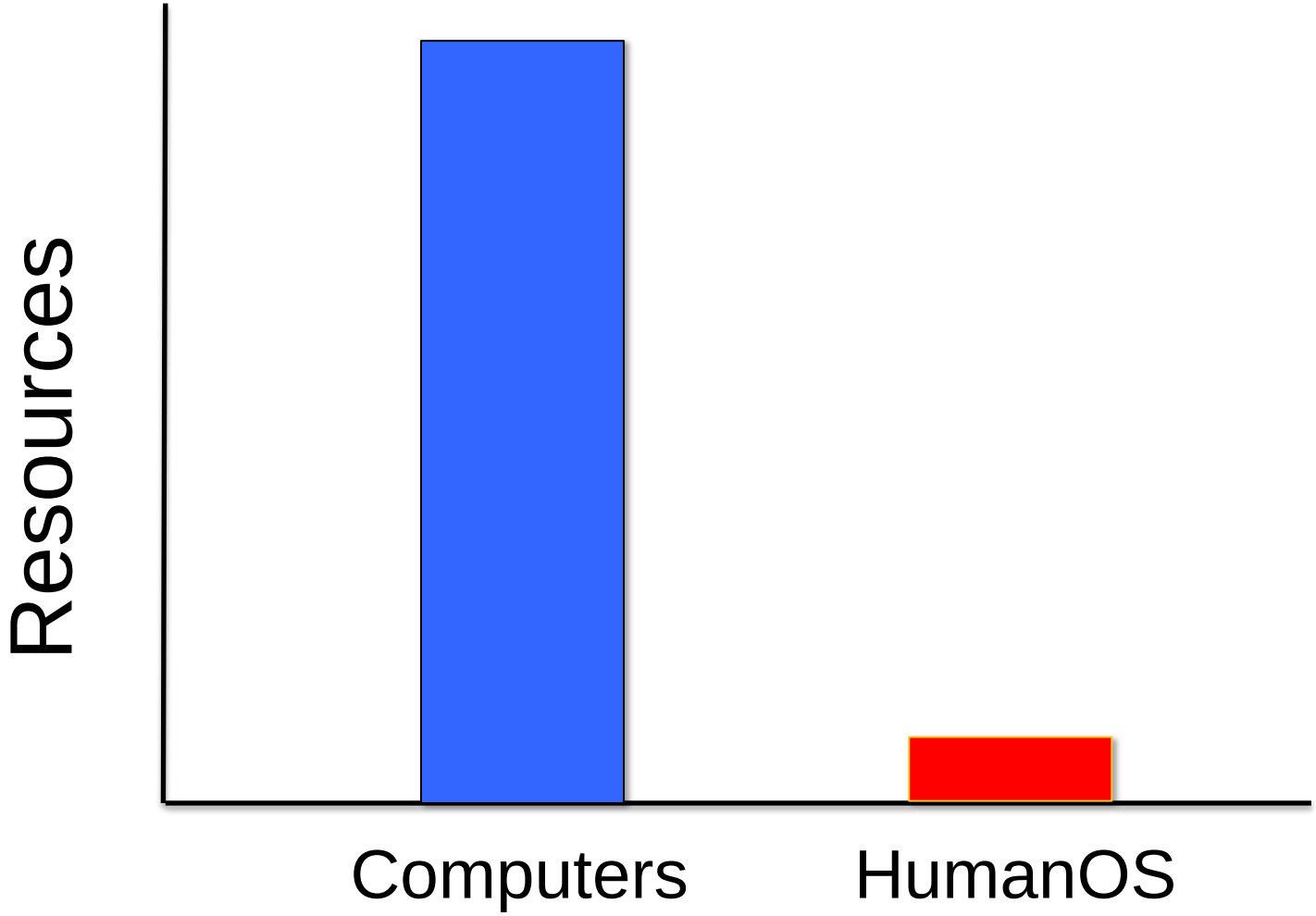


MITIGATING THE TOP HUMAN RISKS

Lance Spitzner
SANS Securing The Human

Session ID: HUM-W25
Session Classification: Intermediate




Resources
Computers
HumanOS

1 in 251,800,000

1 in 112,000,000

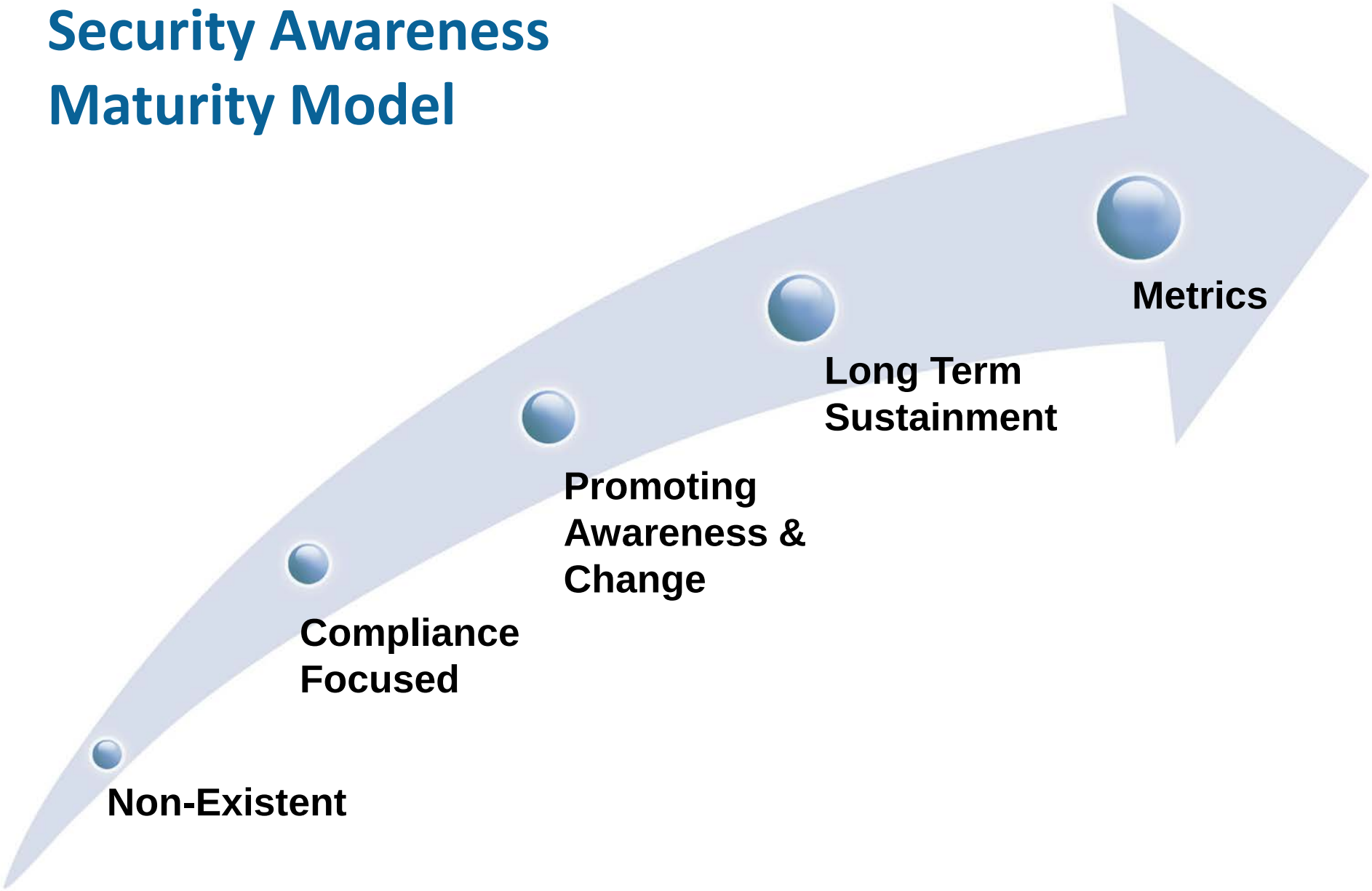
Top 7 Human Risks

- Community Analysis
  - Carnegie Mellon University
  - iSightPartners
  - MITRE
  - SecureWorks
  - Mandiant
  - Virginia Tech
- Phishing / Spear Phishing
- Password reuse
- Unpatched or poorly configured devices (BYOD)
- Mobile media
- Data leakage via Social Networking
- Lack of situational awareness
- Accidental disclosure / loss

Common Misconceptions

- Awareness does not work
- Someone always falls victim
- Awareness is only about prevention

Security Awareness Maturity Model



Security Awareness Roadmap

Just like computers, people store, process, and transfer information. However, very little has been done to secure this "human" operating system, or HumanOS. As a result, people rather than technology are now the primary attack vector. Security awareness training is one of the most effective ways to address this problem. This roadmap is designed to help your organization build, maintain and measure a high-impact security awareness program that reduces risk by changing people's behavior and also meets your legal, compliance, and audit requirements. To use this roadmap, first identify the maturity level of your security awareness program and where you want to take it. Then follow the detailed steps to get there.

1 No Awareness Program

Program does not exist. Employees have no idea that they are a target, do not know or understand organizational security policies, and easily fall victim to cyber or human-based attacks.

2 Compliance Focused

Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc basis. Employees are unsure of organizational policies, their role in protecting their organization's information assets, and how to prevent, identify, or report a security incident.

How To Get There:

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards, which will likely require coordination with compliance or audit officer.
- Develop or purchase training to meet those requirements.
- Deploy security awareness training.
- Track who completes training, and when.

Deliverables:

- Annual training materials such as videos, newsletters and on-site presentations.
- Reports of who has and who has not completed required training.

Standards Requiring Awareness Training

- ISO/IEC 27002 §8.2.2
- PCI DSS §12.6
- SOX §404(a).(a).(1)
- GLBA §6801.(b).(1).(3)
- FISMA §3544.(b).(4).(A),(B)
- HIPAA §164.308.(a).(5).(i)
- NERC §CIP-004-3(B)(R1)
- EU Data Protection Directive

3 Promotes Awareness & Change

Program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors and staff understand and follow organizational policies and actively recognize, prevent and report incidents.

How To Get There:

- Begin by identifying stakeholders in your organization. These are the individuals who are key to making your program a success. Once identified, build and execute a plan to gain their support. Methods to gain support include a human risk survey, awareness assessments, root cause analysis of recent incidents, industry reports or cost-benefit analysis.
- Create a baseline of your organization's security awarenes level, such as with a human risk survey or phishing assessment. For additional examples refer to the Metrics section.
- Create a Project Charter that gives you authorization to begin the planning process. The Project Charter should set key expectations including identifying the project manager, cost estimates, program scope, goals, milestones, and assumptions.
- Have management review the Project Charter. Once it is approved, planning can officially begin.
- Establish a Steering Committee to assist in planning, executing, and maintaining the awareness program. Steering Committee should include 5-10 volunteer advisors from different departments or business units within your organization.
- Identify WHO you will be targeting in your program. Different roles may require different or additional training, including employees, help desk, IT staff, developers, and senior leadership.
- Identify WHAT you will communicate to the different groups targeted by your program. The goal is to create the shortest training possible that has the greatest impact. Begin with a risk analysis to identify the different human-based risks to your organization, document those risks in a matrix, and then prioritize the risks from high to low. Then select which risks you will address in your program based on priority level, time restrictions and other organizational requirements. Create a separate Learning Objectives document for each topic that identifies the different behaviors you need to change.
- Once you have determined WHO is the target of your awareness program and WHAT you will teach them, determine HOW you will communicate that content. To create an engaging program focus on how people will benefit from the training, how most of the lessons apply to their personal lives. There are two categories of training: Primary and Reinforcement. Primary training teaches new content and is usually taught annually or semi-annually and either onsite or online. Reinforcement training is employed throughout the rest of the year to reinforce key topics. Common examples of reinforcement training include newsletters, posters, podcasts, assessments and blogs. When teaching a specific topic, refer to that topic's Learning Objectives document to determine what content to communicate. This way regardless of the different ways you communicate a topic, the message will always be consistent.
- Create an execution plan in coordination with your Steering Committee. The plan should begin with WHY you are launching a security awareness program and its goals and overall scope. Then document WHO you will target in your awareness program, WHAT you will teach them and HOW. Include a timeline that identifies key milestones and the launch date of the program, critical resources involved and any other relevant information your organization may require for planning purposes.
- Have management review the plan. Once the plan is approved, you can execute your awareness program. Have the most senior stakeholder (such as your CEO) announce the program to the organization, such as by email, blog posting, or taped video.

Deliverables:

- Stakeholder matrix
- Gaining stakeholder support presentation
- Human risk survey
- Project Charter
- Steering Committee matrix
- Topics matrix
- Learning objectives document for each topic
- Execution plan

4 Long-Term Sustainment

Program has processes and resources in place for a long-term life cycle, including at a minimum an annual review and update of both training content and communication methods. As a result, the program is an established part of the organization's culture and is current and engaging.

How To Get There:

- Identify when you will review your awareness program each year.
- Identify new or changing technologies, threats, business requirements, or compliance standards that should be included in your annual update.
- Conduct an assessment of your organization's security awareness level and compare that to the baseline taken in stage 3.
- Survey staff for feedback, including what elements they liked best about the program, what needs to be changed, which topic they found most interesting, and which behaviors they changed.
- Review all the topics you are communicating and identify if new topics need to be added, and which existing topics should be removed or updated.
- Once topic changes have been identified, review and update the learning objectives for each topic.
- Review how the topics are communicated, which methods have had the greatest impact, and which need to be updated or dropped.
- Conduct an annual review and update of the budget to address changing business objectives.

Deliverables:

- Content tracking matrix used to document which topics and learning objectives were updated, by whom, and when.

5 Metrics Framework

Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. In addition, some set of metrics will be used in previous stages.

How To Get There:

- Identify key metrics that relate to business outcomes.
- Document how and when you intend to measure the metrics.
- Identify who to communicate results to, when, and how.
- Execute metrics measurement.

Deliverables:

- Metrics matrix

Examples of Metrics:

- No. of people who fall victim to monthly phishing assessments.
- No. of monthly infected systems.
- No. of monthly incidents reported.
- No. of people who completed the awareness training.
- No. of weak or shared passwords.
- Employee scores from before/after testing.
- % of users sampled with positive attitude towards information security.
- % of users sampled who believe their actions can have an impact on security.

Additional Materials:

- **NIST SP800-50**
  Building an Information Technology Security and Training Program
- **ENISA Awareness Guide (2010)**
  How to Raise Information Security Awareness
- **20 Critical Controls**
  Twenty Critical Security Controls for Effective Cyber Defense

About the Poster

This roadmap was developed as a consensus project by security professionals actively involved in security awareness programs. If you have any suggestions or would like to get involved please contact community@securingthehuman.org

Contributors Include: Randy Marchany (Virginia Tech), Cortney Stephens (Union Gas), Julie Sobel (Alliance Data), Tonia Dudley (Honeywell), John Andrew (Honeywell), Pieter Danhieux (BAE Systems Detica), Vivian Gernand (Corning), Christopher Ipsen (State of Nevada), Jenn Lesser (Facebook), Mark Merkow (PayPal), Sam Segran (Texas Tech University), Tracy Grunig (Arizona State University), Geordie Stewart (Risk Intelligence), Greg Aurigemma (Flight Safety), Janet Roberts (Progressive Insurance), Chris Sorensen (GE Capital), Mary Naphen (Lincoln Financial Group), David Vaughn (HP Enterprise Services), Tim Harwood (BP), Tanja Craig (BP), Dave Piscitello (ICANN), Eric Phifer (Seacost National Bank), Antonio Merola.

Documents followed by this icon may be downloaded at:
www.securingthehuman.org/resources/planning

Project Charter

- Who is in charge?
- What is the scope?
- What are you specific goals?
- When will training start?

Steering Committee

- Team of 5-10 volunteers to build, maintain and measure your program.
- Not only guides but ambassadors.
- Have a mix of departments and roles.
- Can meet and coordinate virtually (maillist).

WHO

- Who are you targeting in your program. Different targets often require different training.
  - Employees / contractors
  - IT Staff / Developers / Database admins
  - Help Desk
  - Senior management

WHAT

- Use a modular approach for your awareness training. Each awareness topic is a separate module, each with its own learning objectives.
- Goal is to teach the fewest topics that have the greatest impact.
  - You are a target
  - Phishing / Spear Phishing
  - Password reuse
  - Keep devices updated
  - Mobile media
  - Data leakage via Social Networking
  - Accidental disclosure / loss

HOW

- This is where most programs fail, you need to engage. Goal is training so valuable employees ask how their family/friends can take it.
  - Focus on how people benefit. 75% of your topics apply to both personal and work lives.
  - Focus on how you are enabling technology.
  - Create content people can consume on their own schedule.
- Training should be continuous throughout the year (patch management for the HumanOS)


SANS

SANS SECURING THE HUMAN

OUCH! | December 2012

Seven Steps to a Secure Computer

when you do connect to the Internet, your new computer is protected behind a firewall or home Wi-Fi access point. In addition, most computer operating systems, including Windows and OS X (and even many applications), have an automatic updating feature built-in. Enable automated updating to check for updates at least once a day; this helps ensure your computer will remain updated and secure. If a vendor releases a patch that you have to manually install, be sure to install it as soon as possible.

3. SECURITY SOFTWARE

Once your computer is updated you want to ensure you have security software installed and enabled. The two most common types of security software are anti-virus and firewalls. Anti-virus helps identify infected files you may have downloaded or shared with others and stops these malicious files from harming your computer. Firewalls act like a virtual policeman; they determine who can and cannot talk to your computer. Many security vendors now offer entire security software suites that include firewall, anti-virus and other software options. You may want to consider purchasing an entire security package.

By following these simple steps you can help ensure a secure computer.

This way you can apply different controls to each user (such as parental controls for your children) and track who did what. In addition, grant each user the minimum privileges they need to use the computer. Never give someone administrative access unless they absolutely need it, including yourself. Only use administrative privileges when you need them, such as to install software or changing a system configuration.

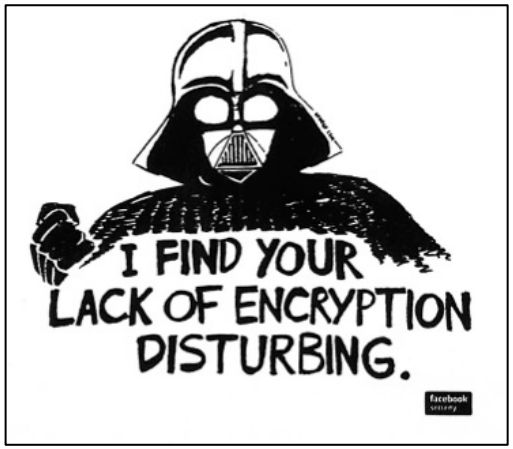
4. ACCOUNTS

Every person that has authorized access to your computer should have their own separate account protected by a unique, strong password. Never share accounts. If this is a personal computer for home use, create a separate account for each member of your own family, especially children.

5. SECURITY ON THE GO

If your computer is portable, such as a laptop, you may want to consider full disk encryption (FDE). Encryption helps ensure that the data on your computer is protected even if you lose it. You may also want to ensure the computer screen is password locked, so people cannot

 http://www.securingthehuman.org



Deployment Plan

- Once you answer key questions including WHO, WHAT & HOW put together draft plan with Steering Committee.
- Have management review, update and approve plan.
- Execute plan.

Update Content

- Your technology, business requirements, and threats are constantly changing.
- Update content at least once a year with Steering Committee.

Metrics That Measure the Impact of Your Program

Metric Name	What Is Measured	How It is Measured	When Is It Measured	Who Measures?	Details
Phishing Awareness	Number of people who fall victim to a phishing attack	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 Detection	Number of people who detect and report a phishing attack	Phishing assessment	Monthly	Security team	Using 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.
Infected Computers	Number of infected computers.	Help desk or centralized AV management software.	Monthly	Help desk or security team.	Most infected computers are a result of human behavior (infected attachments, malicious links, etc.). As employees are trained this number should go down over time.
Awareness Survey	Number of employees understand and are following security policies, processes and standards	Online Survey	Bi-annually	Security team or HR	Employees take a survey on 25-50 questions that determine understanding and following of policy. Questions can include if people share passwords, know how to contact security, and if they have been hacked.
Behavior Survey	Top lessons employees have learned and top behaviors changed because of this.	Online survey	Bi-annually	Security team or human resources	This survey is not interested in peoples' understanding of policies. Instead we want to collect what are the key points people are taking away from the training, what are the most common behaviors we are changing.
Employee Feedback	Do employees like the training, are they engaged? If they do not like the training your program will not have an impact.	Online Feedback Forms	Bi-annually	Security team or human resources.	The ultimate goal is to create training that not only people want to take, but training they want to share with others. If you have employees asking if their family can take the training, you have created a truly engaging program.
Testing	Number of employees understand security expectations, specifically the behaviors they should change and how.	Online Testing	Bi-annually	Security team or HR	Questions that specifically test knowledge of security awareness training. Specifically if they know what behaviors they need to change and how.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walk through	Monthly or weekly	Information security or physical security team	Security team does walk through of organizational facilities checking each desktop or separate work environment. Looking to ensure that individuals are following organizational desktop policy.
Passwords	Number of employees using strong passwords.	Password brute forcing.	Monthly or quarterly	Security team	Security gains authorized access to system password database (such on AD or Unix server) and attempts to brute force or crack password hashes.
Social Engineering	Number of employees who can identify, stop and report a social engineering attack.	Phone call assessments	Monthly	Security team	Security team calls random employees attacking as an attacker would and attempting to social engineer the victim. Example could be pretending to be Microsoft support and having victim download infected anti-virus.
Sensitive Data	Number of employees posting sensitive organizational information on social networking sites.	Online searches for key terms	Monthly	Security team (or outsource)	Do extensive searches on sites such as Facebook or LinkedIn to ensure employees are not posting sensitive organizational information.
Data Wiping	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping.	Random	Information security or physical security	Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures.

NOTE: *These metrics are used to measure the impact of your security awareness program. Specifically how employee understanding and behavior has changed. This is used to measure value of the program, including reducing costs and risk. For more resources visit http://www.securingthehuman.org/resources/planning*

Key Lessons Learned

- Give yourself time for planning (1-3 months)
- Don't try everything at once, you have years to develop your program
- If people do not like the training it will fail
- Share success stories

Summary

- Humans are another operating system, one that nothing has been done to secure to date.

- By taking some basic steps you can go a long way in securing people by changing key behaviors.

Free Community Resources

- Awareness Roadmap & Program Planning Kit
- Phishing Planning Kit
- Monthly OUCH! awareness newsletter
- Monthly awareness video
- Awareness presentations & posters
- Resources for gaining management support

www.securingthehuman.org/resources