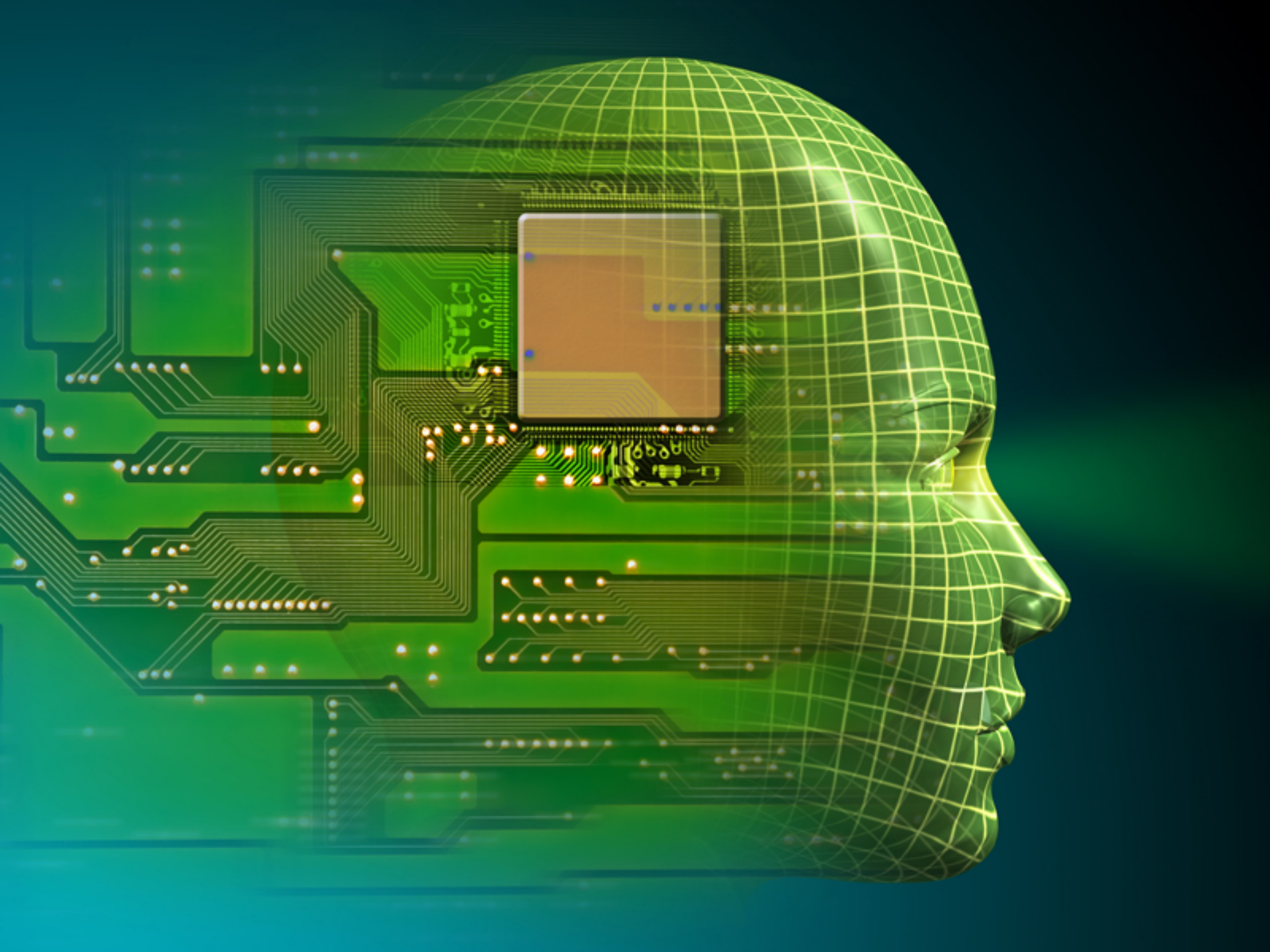
SECURING THE HUMAN



1 in 251,800,000

Source: http://www.bookofodds.com/content/view/full/252163

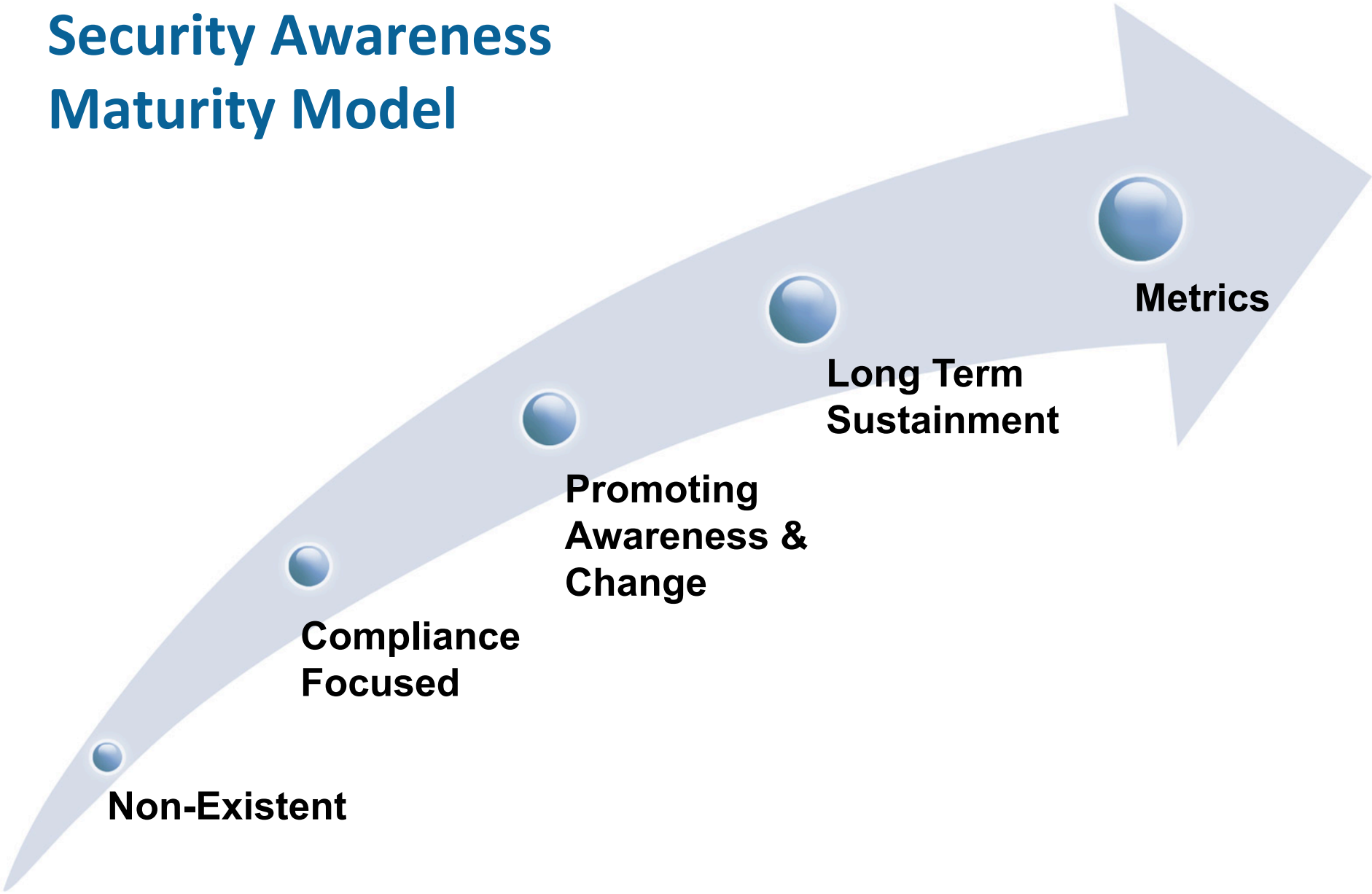
1 in 112,000,000

Source: http://www.bookofodds.com/content/view/full/248157

Key Points on Awareness

- Most awareness programs have had little impact because they were never designed to.
- Awareness is simply another control.
- Long term program – lifecycle.
- Not just prevention – detection and response.

Security Awareness Maturity Model



Steering Committee

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

The Plan

Once you form your Steering Committee you need a plan to ensure greatest impact of your program.

- Who
- What
- How

Who

WHO determines who is the target of your program. Different targets may require different training.

- Employees / Contractors
- Faculty / Students
- Families / Kids
- IT Staff / Help Desk / App Dev

Security Awareness Training Modules


You Are A Target


Social Engineering


Email & Instant Messaging


Browsing

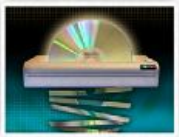

Social Networking


Mobile Device Security


Passwords


Encryption


Data Protection


Data Destruction


Wi-Fi Security


Working Away From Office


Insider Threat


Help Desk


IT Staff

Physical Security


Protecting Your Personal Computer


Protecting Your Home Network


Protecting Your Kids Online


Hacked


Senior Management

Compliance Training Modules


PCI DSS


FERPA


HIPAA


Personally Identifiable Information (PII)


Criminal Justice

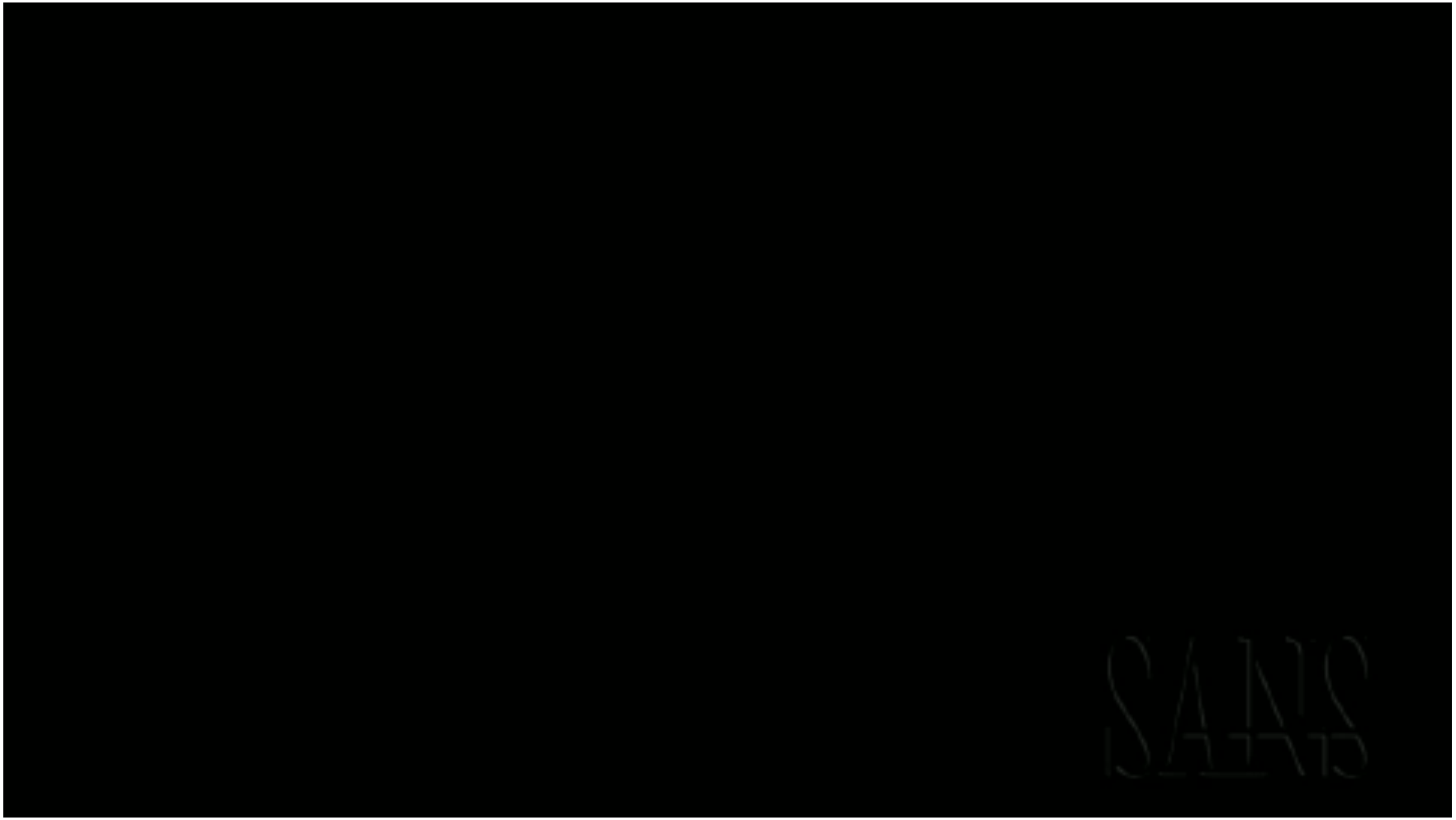

Federal Tax

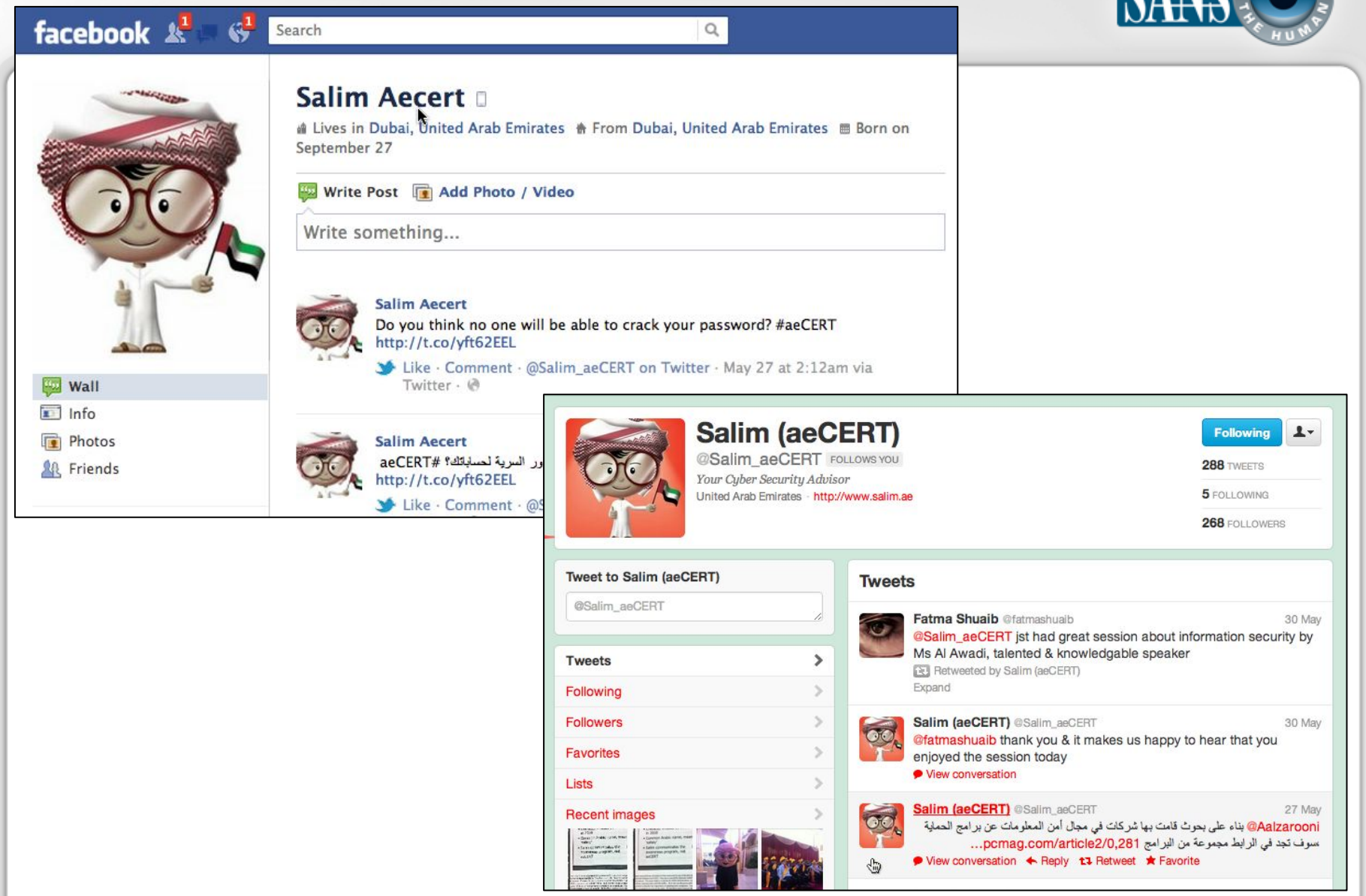
GLBA-EDU

GLBA-FIN

Engage

- Focus on how they benefit, 70-80% of your awareness program also applies to peoples' personal life.
- Do not focus on Fear, Uncertainty and Doubt, instead focus on how you enable the use of technology.
- Take on their own time.


SANS


facebook
Search
Salim Aecert
Lives in Dubai, United Arab Emirates From Dubai, United Arab Emirates Born on September 27
Write Post
Add Photo / Video
Write something...
Wall
Info
Photos
Friends
Salim Aecert
Do you think no one will be able to crack your password? #aeCERT
http://t.co/yft62EEL
Like · Comment · @Salim_aeCERT on Twitter · May 27 at 2:12am via Twitter
Salim Aecert
http://t.co/yft62EEL
Like · Comment
Salim (aeCERT)
@Salim_aeCERT FOLLOWS YOU
Your Cyber Security Advisor
United Arab Emirates · http://www.salim.ae
Following
288 TWEETS
5 FOLLOWING
268 FOLLOWERS
Tweet to Salim (aeCERT)
@Salim_aeCERT
Tweets
Following
Followers
Favorites
Lists
Recent images
Tweets
Fatma Shuaib @fatmashuaib 30 May
@Salim_aeCERT jst had great session about information security by Ms Al Awadi, talented & knowledgable speaker
Retweeted by Salim (aeCERT)
Expand
Salim (aeCERT) @Salim_aeCERT 30 May
@fatmashuaib thank you & it makes us happy to hear that you enjoyed the session today
View conversation
Salim (aeCERT) @Salim_aeCERT 27 May
@Aalzarooni بناء على بحوث قامت بها شركات في مجال أمن المعلومات عن برامج الحماية سوف تجد في الرابط مجموعة من البرامج pcmag.com/article2/0,281...
View conversation Reply Retweet Favorite

Blog


If you're ready for a zombie apocalypse, then you're ready for any emergency
emergency.cdc.gov
CDC

Update Content

- Technology, threats and standards are constantly changing.
- Update content at least once a year.
- You and steering committee need to review and update training.
- Ensure you have budget allocated for updates.

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*

Phishing Assessments

From: Systems Administrator
Subject: Message Undelivered: Password Change
Date: September 22, 2010 1:39:20 AM CDT
To: Victim <victim@example.com>

Your message did not reach some or all of the intended recipients.

Subject: Password Change
Sent: 9/22/10 01:35 AM

The following recipient(s) could not be reached: victim@example.com

The email system was unable to deliver the message, but did not report a specific reason. Check the address and try again. If it still fails, contact your system administrator. mail.example.com #5.0.0 smtp; 5.1.0 - Unknown address error 550'5.1.1 unknown or illegal alias: (delivery attempts: 3)

Click here if you can't see the text

Free Resources

- Awareness program planning kit
- Phishing assessment planning kit
- Monthly OUCH! awareness newsletter
- Awareness presentations
- Business justification
- Free trial of full awareness library

www.securingthehuman.org/resources

Security Awareness Roadmap

This roadmap is designed to help your organization build and maintain a high-impact security awareness program that not only meets all your legal and compliance requirements, but reduces risk in your organization by changing behaviors. The best way to leverage this roadmap is identify the maturity of you current awareness program, where you want your program to go, and then follow the steps to get there. On the back of this poster are the eight key steps and respective documents to building a high-impact security awareness program.

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 standards to which your organization must adhere
- Identify security awareness requirements for those standards
- Develop or purchase training to meet those requirements
- Deploy security awareness training
- Track who completes the training, and when

Deliverables:

- Annual training materials such as videos, newsletters, 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)
- CobiT §PO7.4 & §DS7
- FISMA §3544.(b).(4).(A).(B)
- HIPAA §164.308.(a).(5).(i)
- NERC §CIP-004-3(B)(R1)
- US State Privacy Laws
- EU Data Protection Directive

3 Promoting 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 are aware of organizational policies and actively recognize, prevent and report incidents.

How To Get There:

- Create a Project Charter that identifies project manager, estimates costs, defines program scope, goals and objectives. In addition Project Charter justifies the program based on the business mission, identifies key milestones, and sets assumptions and constraints.
- Have management review and approve Project Charter. Once approved planning can begin.
- Identify key stakeholders, including champions and blockers, and gain their support
- Establish Steering Committee, 5-10 advisors from organization who assist in planning, deploying and maintaining your program
- Identify WHO you will target in your program, WHAT you will communicate to them, and HOW you will communicate the training to them
- Develop an execution plan in coordination with steering committee that includes WHO, WHAT and HOW and timeline for events.
- Once finalized have management review the execution plan, once approved you can launch your awareness program.
- Establish awareness baseline, determine the awareness level of your employees and how vulnerable they are to human based attacks.

Deliverables:

- Project charter
- Steering Committee matrix
- Security awareness baseline survey
- Training topics matrix that identifies key topics
- Learning objectives document for each topic
- Communications plan
- 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 becomes an established part of the organization's culture and is always 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
- Review all topics you are communicating and identify if new topics need to be added, which existing topics should be removed, and which existing topics need to be updated
- Once topic changes have been identified, review and update the learning objectives for each topic
- Review how the topics will be communicated, which communication methods had the greatest impact and which need to updated or no longer used.
- Annual review and update of budget, to include changing business objectives

Deliverables:

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

5 Metrics

Program has metrics in place to track progress and measure impact. As a result program is continuously improving and able to demonstrate return on investment.

How To Get There:

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

Deliverables:

- Metrics matrix

Metric Examples:

- # of people who fall victim to monthly phishing assessments
- # of monthly infected systems
- # of monthly incidents reported
- # of people who completed the awareness training
- # of weak or shared passwords
- Employee scores from before/after testing

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
- **NIST SP800-53**
  Recommended Security Controls for Federal Information Systems and Organizations

Community Project

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 stratsec), Vivian Gernand (Corning), Christopher Ipsen (State of Nevada), Jenn Lesser (Facebook)

An example of this document can be downloaded from www.securingthehuman.org/resources/planning