Designing and developing an effective Security Awareness and Training program

Meenu Gupta,CISA,CISM,CISSP,CIPP
President
Mittal Technologies
Meenu.gupta@Mittal-Tech.com

Agenda

- Defining Security Awareness Training
- Why is it important
- Doing it correctly
- **The Solution**
- Questions

Defining Security Awareness Training

From the Internet….

“……raising awareness on critical security issues”

“*Our all-inclusive turn-key, enterprise security awareness program trains your employees to protect your network against security breaches and keeps them security aware through ongoing awareness programs. …“*

“An active security awareness program can greatly reduce many risks which cannot be addressed through security software and hardware devices. In these cases, it's the human element of security that must be addressed which is exactly what our products are designed to do.”

Defining Security Awareness Training

National Institutes of Standards and Technology (NIST)

Public Law 100-235 titled, "The Computer Security Act of 1987," mandated NIST and OPM to create guidance on computer security awareness and training based on functional organizational roles. Guidance was produced in the form of NIST Special Publication 800-16 titled, "*Information Technology Security Training Requirements: A Role- and Performance-Based Model*." The learning continuum modeled in this guidance provides the relationship between awareness, training, and education. The publication also contains a methodology that can be used to develop training courses for a number of audiences which may be deemed to have significant information security responsibilities. In October 2003, NIST also published Special Publication 800-50 - "Building an Information Technology Security Awareness and Training Program."

Awareness
...to focus attention on security

Training
...to produce relevant and needed security skills and competency

Education
...to integrate all (security skills and competencies) into a common body of knowledge, adding a multidisciplinary study of concepts, issues, and principles

Professional Development (Organizations and Certifications)
...imply a guarantee as meeting a standard by applying evaluation or measurement criteria

Defining Security Awareness Training

ENISA (European Network and Information Security Agency)

The Information Security Forum (ISF) is one of the world's leading independent authorities on information security. Through surveys and research, the ISF have defined information security awareness as:

> **'an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behavioral change.'**

Defining Security Awareness Training Objectives

- ← Communicate risks and vulnerabilities facing the business environment
- ← Communicate company objectives regarding security and enterprise risk.
- ← Communicate company policies & procedures regarding security and enterprise risk
- ← Communicate organization roles and responsibilities
- → **Invite audience input**
- → **Invite audience feedback**
- → **Invite audience ideas**
- ← Provide resources and tools for deeper knowledge
- ← Provide a mechanism for on-going communication on issues related to risks and vulnerabilities

Defining Security Awareness Training

Security Awareness training is the process of educating people about:

- the risks and vulnerabilities facing their business environment
- the tools they can use to minimize these risks and vulnerabilities
- the mechanisms a company has in place by which people are able to keep their knowledge current.

Why is it important?

The People Factor[1]

We already have

- Management Controls
- Technical Controls
- Operational Controls

We need

- Human Controls

1 – Source: NIST

Why is it important?

Risk mitigation through creating:

- Awareness of confidentiality, availability, and integrity risks that face the business
- Awareness of vulnerabilities that affect computing systems users interact with
- Knowledge of corporate policies and procedures designed to address these risks
- Understanding of roles and responsibilities

Why is it important?

Also, it is an opportunity to:

- Hold an enterprise-wide discussion on risk.
- Get security out of the inner sanctums of IT and into the hands of the end user
- Create an environment that constantly reminds people of the “right thing” to do

If we can get the user to say “what role can I play” that’s a sign of success!

Doing it Right

Myth:

Security Awareness training will teach users about security.

Problem:

Most security awareness programs are hastily created PowerPoint slides

Challenge:

Creating a program that is relevant, effective and entertaining

A Bigger Challenge:

Making this program a part of your organizational processes and keeping it updated

Solution

1. Establish realistic goals for the organization
2. Design the program
3. Develop the training
    I. Establish criteria for success
    II. Get executive buy-in
4. Implement the training
    I. Make it a part of the organization processes
    II. Measure effectiveness

Goals

Wrong!

1. It is mandatory!
2. Teaching employees about security
3. Making employees aware of security

How about?

1. Proper handling of sensitive information
2. Reduction in internet usage for personal purposes
3. Adherence to password policies
4. Preparedness for contingency events

Make security relevant!

Designing the Program

1. Formal Training
    1. Self-paced, Computer based
    2. Instructor Led
    3. Educational conferences
2. Informal Training
    1. Knowledge sharing
    2. Presentations on key topics
    3. Roundtables
    4. Banners
    5. Self study
    6. Other

Developing the Training

Key Steps

1. Identify a Champion/Owner
2. Identify organization needs
    - Surveys
    - Metrics
    - Events
3. Identify the target population
4. Identify customer needs and if they are part of the target population
5. Identify a team of subject matter experts from Security, Policies, Risk areas
    1. Establish goals
    2. Establish the success criteria
    3. Assist with needs assessment
    4. Choose Awareness Topics

Developing the Training

Key Steps

6. Determine training levels and complexity
    - ✓ Basic
    - ✓ Intermediate
    - ✓ Advanced
7. Determine course length and delivery schedule
8. Determine the delivery vehicle
9. Identify resources for implementation
10. Develop content
    - ✓ Off the shelf
    - ✓ In-house
11. Deploy
12. Track and Measure

Training Levels and Complexity

Basic

- Target Audience – Everyone
- Features
  - Visible risks
  - Everyday security issues
  - Policy focus
  - Broad range of topics
  - Designed to generate discussion
  - See sample training

Training Levels and Complexity

Intermediate

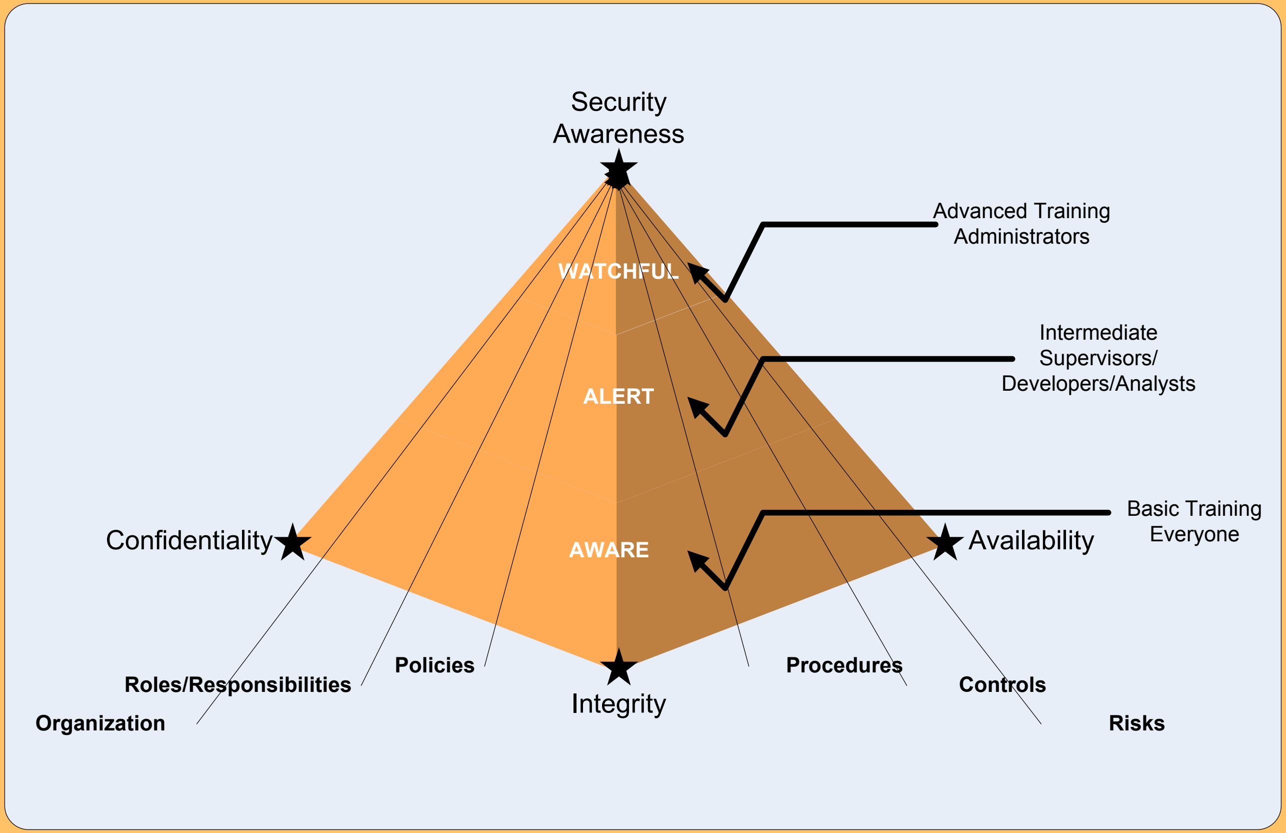
- Target Audience – Management, Developers, Tech Savvy Users
- Features
  - Hidden risks
  - Potential security issues
  - Consideration of security in business processes
  - Consideration of security in SDLC
  - Risk and Controls Framework
  - Policy enforcement
  - Compliance and Audits

Training Levels and Complexity

Advance

- Target Audience – System Administrators, Technical Personnel
- Features
  - Potential vulnerabilities, threats, and risks in computing systems and their mitigation
  - Security Controls
  - Security Policy Settings
  - Security tools
  - Security Log Management
  - Security Reviews

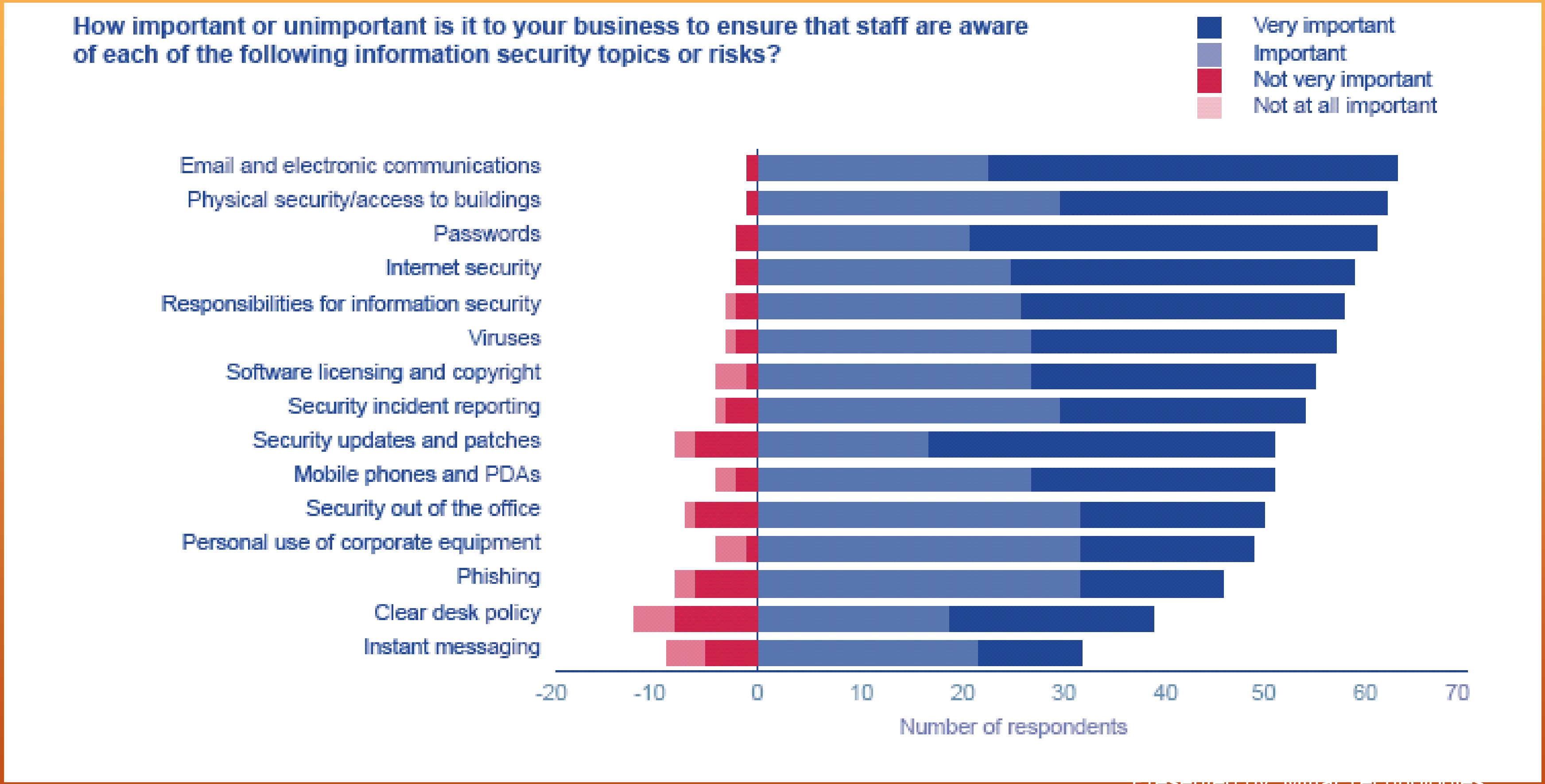
Training Development Model



Sample Security Awareness Training Outline

Basic

Training Content



http://www.enisa.europa.eu

Statement of Training Goals

- **Company recognizes the risks to our business from improper access, loss or stolen business data, or intrusions that can disrupt our computer environments.**

- **Company, a federal contractor, must comply with the FAR -Federal Acquisitions Regulations - which requires that federal contractors be held accountable to the same security standards as the federal government. FISMA (Federal Information Security Management Act) sets the security standards for the federal government and requires that an annual security awareness training be conducted. This training is also required by the Company Corporate Security policy (Information and Technology Policy - Section 4.2).**

- **All Company employees must know Corporate and Company Security policies, controls, and procedures to help them identify and prevent breaches of information security.**

- **Awareness of potential threats and the knowledge of "what we can do about it" is the key to safeguarding our information and our information systems.**

Best practices, rules & regulations, and the company policy require that all Company employees undergo a security awareness training annually.

Sample Training Objectives

- Develop a baseline understanding of common security risks.
- Learn about Company security policies and procedures.
- Learn about “what we can do” to protect company’s information assets.
- Learn about Company Information Security resources that are available to help you with your security related questions.

Sample Topics of Discussion

- Key Security Risks and Controls
  - Access to our buildings and networks
  - Passwords
  - Data Security and Privacy
  - Social Engineering
  - Virus and Intrusion Attacks
  - E-Mail and Internet Access
- Desktop, Laptop, and PDA security
- Business Continuity
- General Security Precautions
- Regulatory Compliance
- Company Contacts
- Quiz

Access To Company Facilities and Networks

Risk: Unauthorized access to our networks or our buildings could result in loss of information assets, interruption of service, or even threat to human lives. We must have appropriate access control procedures to minimize this risk.

There are two types of Access Controls that we follow:

- ❖ Physical Access Controls
  - o Physical access controls prevent unauthorized personnel from getting into Company facilities. They also ensure that the level of physical access is commensurate with the job responsibilities.
  - o All Company personnel must wear their badges all the time.
- ❖ Logical Access Controls
  - o Logical access controls prevent unauthorized personnel from getting into our computer networks or our personal computers. We do this by assigning a user id and password. All logical accesses are controlled by userids and passwords.
  - o Your USERID is your “Identity” and is equal to your “Signature”
    - ✓ Don’t give your identity away
    - ✓ Choose a Secure Password
    - ✓ ………
    - ✓ Log off before you leave your workstation

Passwords

❖ Access control to our networks and computing resources largely relies on the use of userids and passwords. Weak or exposed passwords translate into “no security”. Company follows a password policy that guides how we create and maintain our passwords. It is our responsibility to comply with the Company password policy. Here are a few facts that will help you manage your password.

✓	Maximum password age	99 days
✓	Minimum password age	9 days
✓	Minimum password length	8 characters
✓	Account lockout threshold	9 invalid logon attempts

- ✓ Password needs to be complex and should be a combination of special characters, letters, numbers.

Example of a good password: X@Y3as1

Example of bad passwords: Dictionary words, your UserId, simple sequences such as 123XYZ1, repeating characters

For more information please follow the link to “Password Management Techniques” on

Link…www.company-infosec.com

Data Security and Privacy

"Multiple Security Failures at Veterans Affairs
In the wake of May's massive data theft, the Department of Veterans Affairs falls under the Spotlight. The immense data loss could easily happen again because of weak security at the agency".

"Federal agencies are required to report any suspected privacy breaches to the US-CERT within 1 hour of the breach".

Risk: Not adequately safeguarding our information puts us at risk. These risks could be:

- ✓ Legal risk: Inadvertent or untimely disclosure may have legal ramifications – for example, non-disclosures that we sign with our customers and vendors prohibit us from disclosing certain information without prior written approvals.
- ✓ …..

❖ Not adequately safeguarding our privacy data may lead to identity theft. Identity theft is very real issue which costs time and money to resolve.

Data Security and Privacy

- Additionally, there are many rules and regulations applicable to Company that require us to safeguard our personal and confidential data.
  - ✓ **The Privacy Act of 1974**
  - ✓ **The Health Insurance Portability and Accountability (HIPAA) rule**
  - ✓ **Copyright Protection Act of 1995**
  - ✓ **European Data Protection Act**
  - ✓ **California SB 1386 Privacy Act**
  - ✓ **Cardholder Information Security Program**

- Our company policy requires that:
  - ✓ **Company personnel take accountability for safeguarding confidential data and privacy information**
  - ✓ **Company personnel take accountability for understanding and following appropriate polices and procedures regarding safeguarding information.**
  - ✓ **Company personnel safeguard their computing devices and promptly report lost/stolen devices to their supervisors.**
  - ✓ **Company notify any suspected or detected breach of data privacy to their supervisors immediately.**

Social Engineering

Social Engineering refers to the tactics used to commit internet fraud. It could include people making calls and pretending to be a customer or an employee and trying to gain information on a legitimate customer or employee, or people sending e-mails asking for passwords, credit card numbers or other sensitive information.

Risk: Social engineering could lead to fraudulent transactions or information exposure.

❖ The following guidelines help identify and address social engineering attempts:

➢ If someone is calling on the telephone, but they refuse to give any contact information, that may be an attempt to hide their real identity. If they make a request that's out of the ordinary, that should raise a red flag. If they make a request for something sensitive, you must consult the company policy and verify the authenticity of the caller. You may also consult your supervisor.

➢ If somebody is flattering you, they might be trying to influence you to cooperate. Or they might use an authority ruse--they pretend to have a higher status than you to force information from you.

➢ Never provide your password, account numbers, credit card numbers in the e-mail – personal or business.

➢ Before you enter sensitive information on a web site, make sure it is SSL enabled. Only follow web-links from trusted sources. And always verify URL addresses before visiting a web-site.

What Is a Virus?

A Virus is a software program that attacks our computers in memory or a Hard drive, in E-mail and spreads from one computer to another.

Risk: A virus could delete or corrupt files, or take actions that could be detrimental to our business such as mailing out address lists, causing denial of service by disabling your computer.

- The Company Anti-Virus policy requires that all users have the latest version of Anti Virus Software and virus data files installed.
- It requires periodic checking and continuous monitoring of the computer.
- Company personnel must ensure that the anti-virus software on their computer is running and has up to date signatures.

What Are Symptoms of a Computer Virus ?

- Here is a list of some of the symptoms you may encounter if your computer has a virus.

  - Files disappear.
  - Files replicate.
  - Mystery files appear.
  - Data is transformed or corrupted.
  - Disk space fills up.
  - Computer slows down or locks up.
  - Hard drive crashes.
  - PC is unable to boot.
  - Unusual system messages appear.

  If you observe any of these symptoms, promptly notify the ISC helpdesk. Do not try to eradicate the virus yourself!

E-Mail Usage

E-mail is provided for the purposes of conducting company business. All electronic messages created, stored, and sent over the Company’s network are considered property of the Company.

Risk: Improper use of e-mail could expose our information as e-mails are transmitted in clear text. Sending inappropriate content in the e-mail could expose us to legal and reputational risks.

SENDING E-MAILS

- ❖ Company policy

RECEIVING E-MAILS

- ❖ Company policy

Internet Usage

Company provides Internet access for all employees for business purposes

Risk: Inappropriate use of internet could expose our information or result into hacking attempts against our servers. Unauthorized downloads could compromise the integrity of our network as the downloaded code may be malicious.

Internet / World-Wide Web:

- ❖ The internet is a highly unsecured environment, don’t put anything out there that you wouldn’t mind seeing in the newspaper.

  Some guidelines to keep in mind while on the web:

  - ➢ Don’t post Company or proprietary information on public discussion forums
  - ➢ Don’t download software unless you receive explicit management permission
  - ➢ Text
  - ➢ Text

Desktop, Laptop, and PDA Security

- Only Personal Computing Devices (Personal Computers, MACs, PDAs, other devices with network connection capability, including wireless devices) that meet the following requirements are authorized to connect to the Company Network when:
    - Your Personal Computing Device is in compliance with the current Company hardware and software standards
    - Your Personal Computing Device is running an active anti-virus protection software
    - Text

Desktop, Laptop, and PDA Security

- **Keep your laptop close at hand at all times. Never check it as baggage or put it on luggage carts**
- **Take particular care in high traffic areas such as airports and hotels. Don’t leave your laptop in the car.**
- **Do not store passwords in scripts, as macros, in documents or any electronic file on your laptop**
- **Follow all guidelines about storage of sensitive, proprietary, and software licensing**
- **Ensure appropriate device encryption software is running as approved by the Company Information Security Office.**

Business Continuity

The primary objective of this Business Continuity Plan is to ensure the continued operation of our business by providing the ability to successfully recover critical business functions in the event of a disaster or temporary disruption to the work environment.

- Each Company facility has an active Business Continuity Plan that:
  - Details the course of action that the facility will take
  - Protects and reduces risk to people
  - Minimizes confusion, errors, and expense to the company
  - Reduces loss of services
  - Protects the company assets
- Each employee should know their crisis coordinator
- This information can be found on
- Link…www.company-infosec.com

General Security Precautions

- Question unescorted visitors in your area. Be aware of the actions of the people around you, especially outsiders or unauthorized individuals.
- Report any actual or suspected security incidents to the Help Desk.
- Secure your workstation upon leaving your desk (Press “Ctrl + Alt + Delete”, and then “Lock Computer”)
- Follow clean desk policy. Do not leave confidential documents unlocked or exposed.
- Physical security is an important aspect of managing security. Ensure you are aware of the evacuation procedures at your site. If your site does not have evacuation procedures, notify Company Information Security Office.
- We are all stewards of Company information. If you see areas where our security procedures can be improved, don’t hesitate to contact your Chief Information Security Officer.

Periodically check Company IT Security web site for security news updates:

Company Information Security Office

- ❑ **Responsible for directing the development and enforcement of information assurance and privacy policies in compliance with regulations and standards.**

- ❑ **Supports the corporate security awareness program, corporate …….programs**

- ❑ **Prepares and supports the business for information security audits**

- ❑ **Manages research and development (R&D) activities associated with the information assurance capability**

Company Information Security web site:

Link…www.company-infosec.com

Company Information Security Office

The Information Security Officer (ISO) is:

XXXXXXXX

Company Information Security Office is located in:

XXXXXXXX

Contact Telephone: XXXXXXXX

Contact E-mail: XXXXXXXXXX

Other security resources:

Physical Security

Risk Office

Policy Office

Crisis Management Team

Quiz

1. You should write your password on a sticky note and post to your monitor:

   - ❑ Always
   - ❑ Never
   - ❑ Sometimes

2. If you lost a document that contained company proprietary information you should:

   - ❑ Inform your supervisor
   - ❑ Ask for another copy
   - ❑ Inform the CIO

3. As a team player, if your co-worker is having problems accessing Account Payables application, you should:

   - ❑ Give her your user-id/password to help her
   - ❑ Suggest she contact her supervisor
   - ❑ Suggest she contact the help-desk

Training Feedback

Training was relevant to my job function

- □ Yes
- □ No

Training was enjoyable

- □ Yes
- □ No

I will apply this training to my daily job responsibilities as follows:

Success Factors

1. Senior level buy in
   - ✓ Funding
   - ✓ Empowerment
   - ✓ Support for broad distribution
   - ✓ Executive/senior level messages to staff regarding security
   - ✓ Corporate Governance commitment
   - ✓ Senior Managers attending the training
   - ✓ Senior Management conducting the training
2. Level of attendance at mandatory security forums/briefings.
3. Recognition of security contributions (e.g., awards, contests).

While improved security behavior can result in a decline in incidents or violations, reporting of potential incidents may increase because of enhanced vigilance among users.

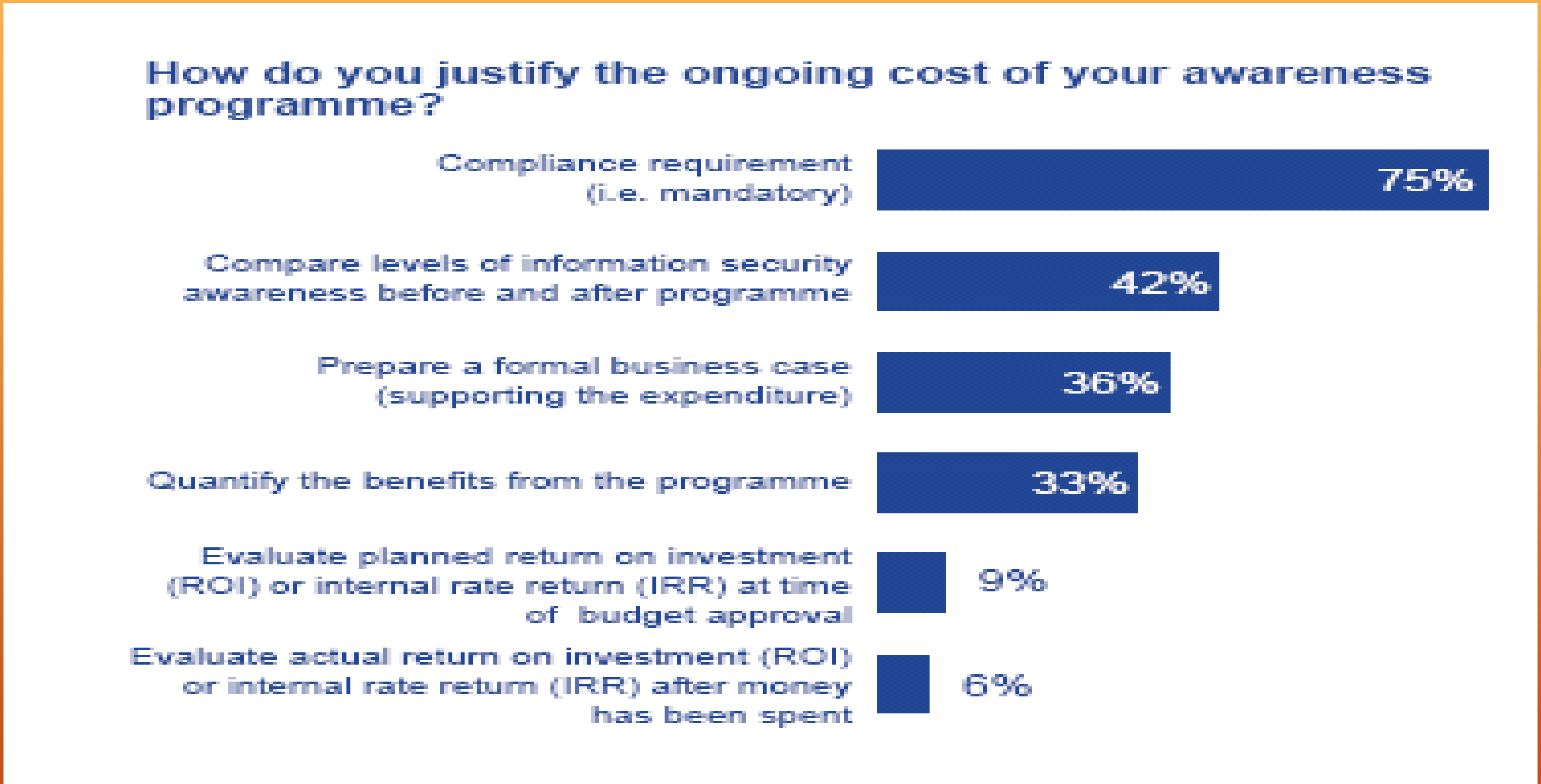
Source: NIST SP 800-50

Resource Estimation

RESOURCE REQUIREMENTS	COST
□ Staffing	$ xxx
□ Contracting Support	$ xxx
□ Facilities	$ xxx
□ Media	$ xxx

Source: NIST SP 800-50

Cost Justification



Presented by: Mittal Technologies

http://www.enisa.europa.eu

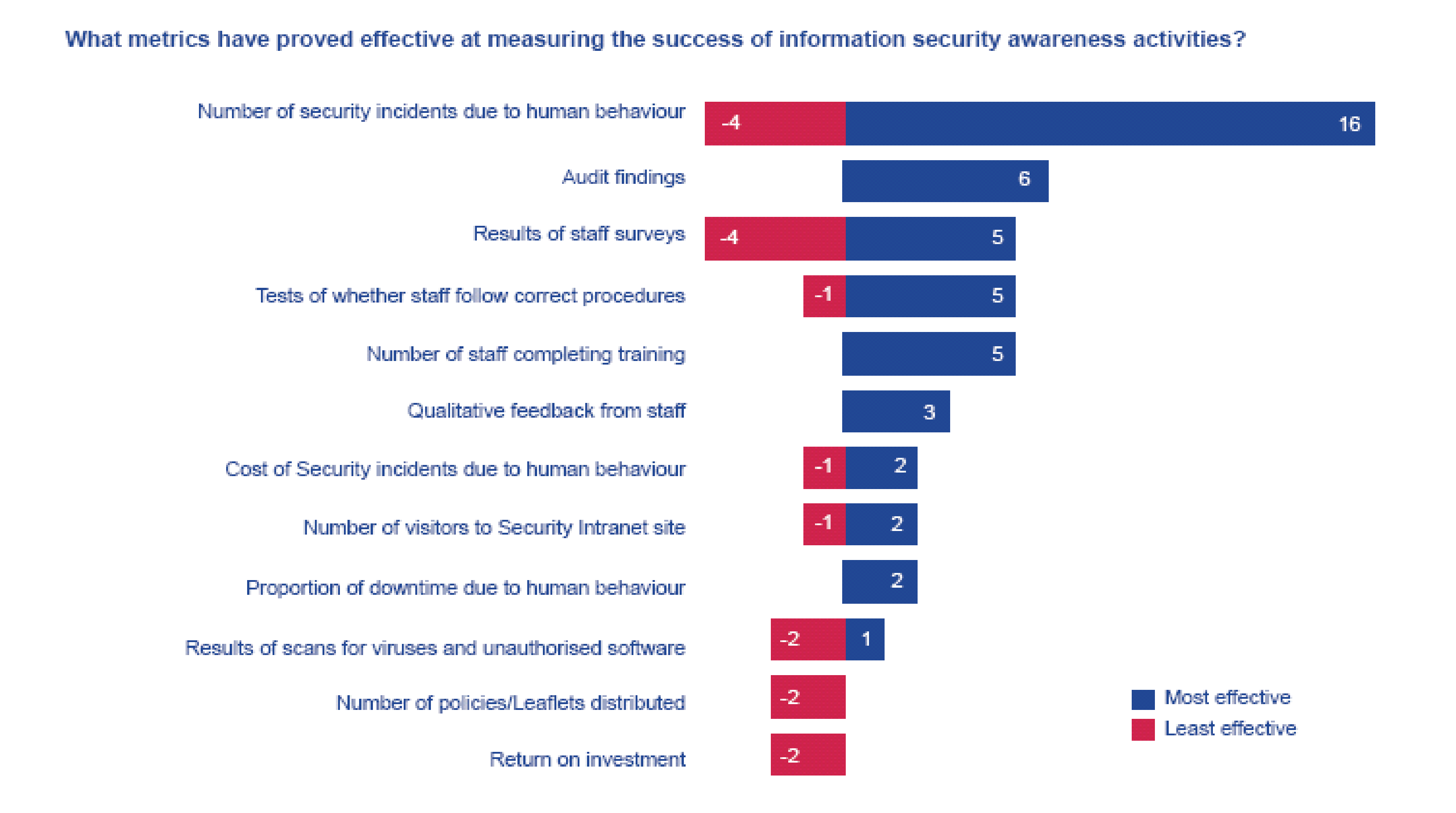
Organization Processes

1. Organizational policy on Security Awareness training
2. Security Awareness during new hire orientation
3. Security Awareness as a performance objective
4. Security Awareness on corporate status reports

Measuring Effectiveness

1. Tracking participation
2. Metrics on incident reports/non-compliance
3. Industry benchmarks
4. Survey feedbacks
5. Feedback from the training sessions

Measuring Success



Presented by: Mittal Technologies

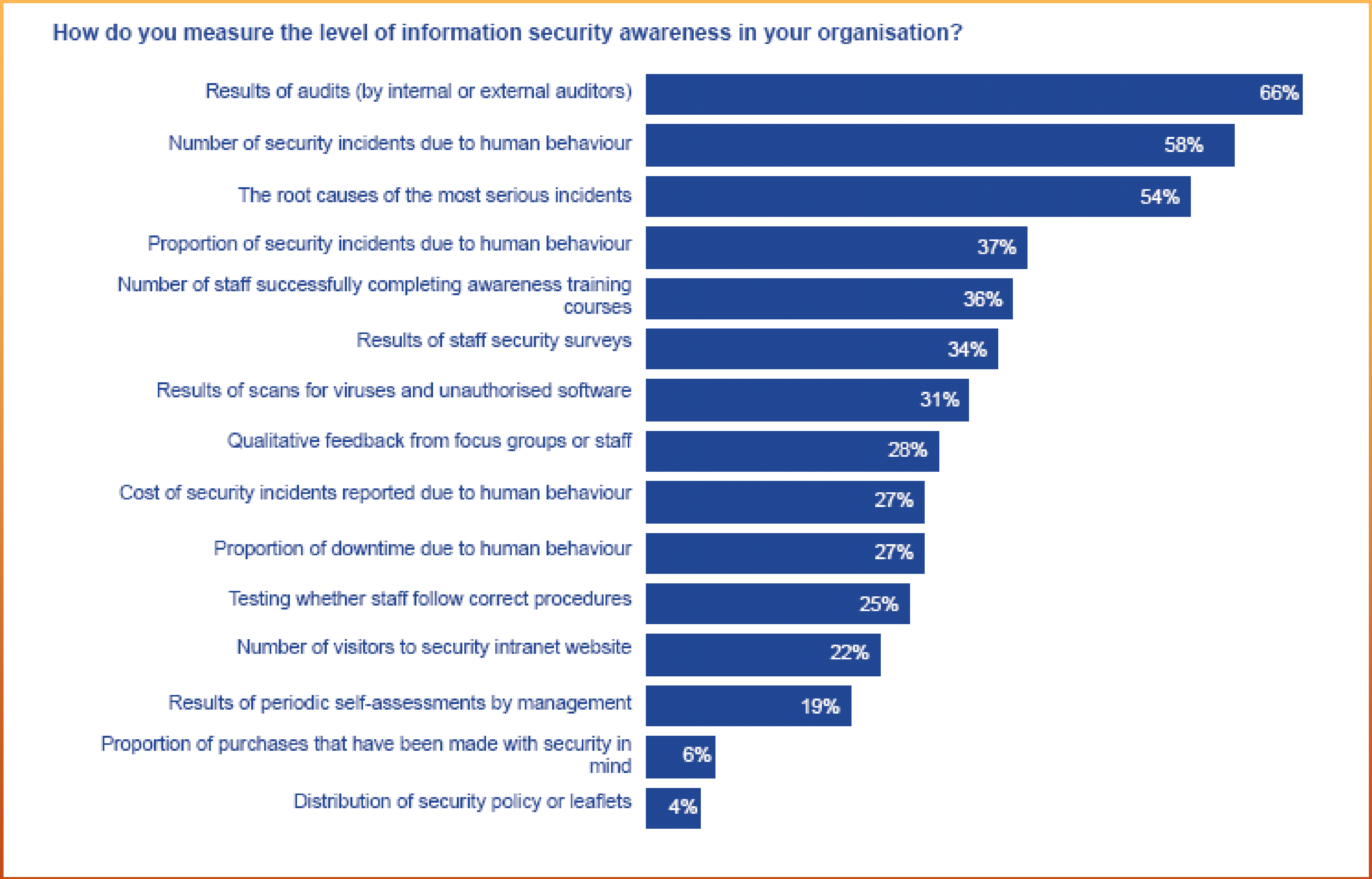
http://www.enisa.europa.eu

Other Considerations

If budget constraints or organizational priorities prohibit development of a formal training program, the following options can be considered:

1. Informal training sessions focusing on specific policies or procedures – brown bags, round tables
2. Specialized training focusing on problem areas – such as data security and privacy
3. Hot topics training – presentations on hot topics
4. PowerPoint presentations

Measuring the Level of Awareness



How do you measure the level of information security awareness in your organisation?

http://www.enisa.europa.eu

Security Awareness topics:

1.Password usage and management – including creation, frequency of changes, and protection

2.Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions

3.Policy – implications of noncompliance

4.Unknown e-mail/attachments

5.Web usage – allowed versus prohibited; monitoring of user activity

6.Spam

7.Data backup and storage – centralized or decentralized approach

8.Social engineering

9.Incident response – contact whom? “What do I do?”

10.Shoulder surfing

11.Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)

12.Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)

13.Handheld device security issues – address both physical and wireless security issues

Source: NIST SP PUB 800-50

Security Awareness topics:

14. Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
15. Laptop security while on travel – address both physical and information security issues
16. Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
17. Timely application of system patches – part of configuration management
18. Software license restriction issues – address when copies are allowed and not allowed
19. Supported/allowed software on organization systems – part of configuration management
20. Access control issues – address least privilege and separation of duties
21. Individual accountability – explain what this means in the organization
22. Use of acknowledgement statements – passwords, access to systems and data, personal use and gain
23. Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity
24. Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems □ Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed
25. E-mail list etiquette – attached files and other rules.

Source: NIST SP PUB 800-50

Questions?