Personnel Security

Kevin Henry CISA, CISSP-ISSMP, SSCP

Pluralsight Author

kevin@kmhenrymanagement.com

People

Weakest link?

Awareness

Types of Attacks

Social Engineering

Ethics

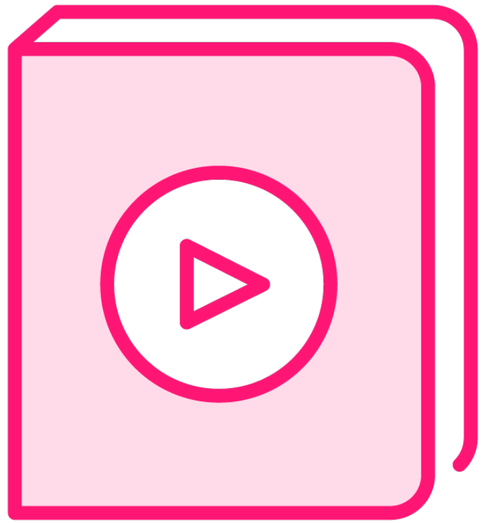
Training and Awareness

We cannot expect a person to know something if they have never been told

NIST SP800-50

Even a small amount of IT security awareness and training can go a long way toward improving the IT security posture of, and vigilance within, an organization.

Awareness

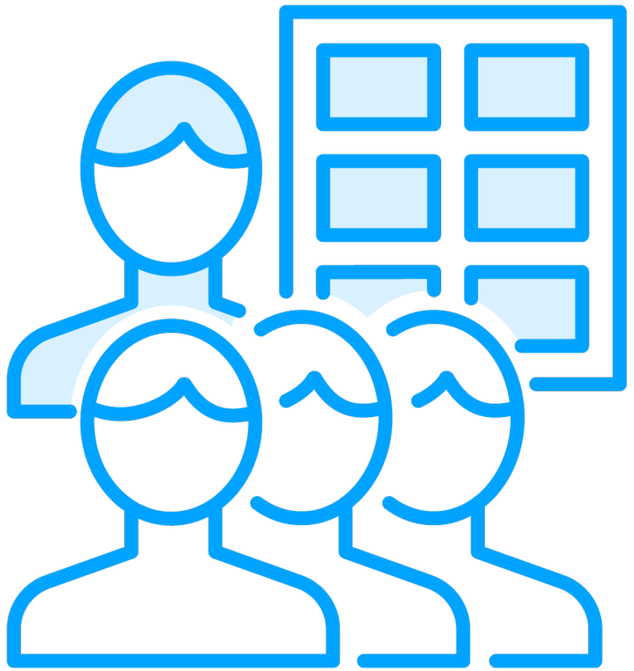


Focused on users

- Rules of behavior
- Policies
- Procedures
- Non-compliance

Management support – lead by example

Awareness Programs



Create accountability

First step in the learning continuum

- Awareness
- Training
- Education

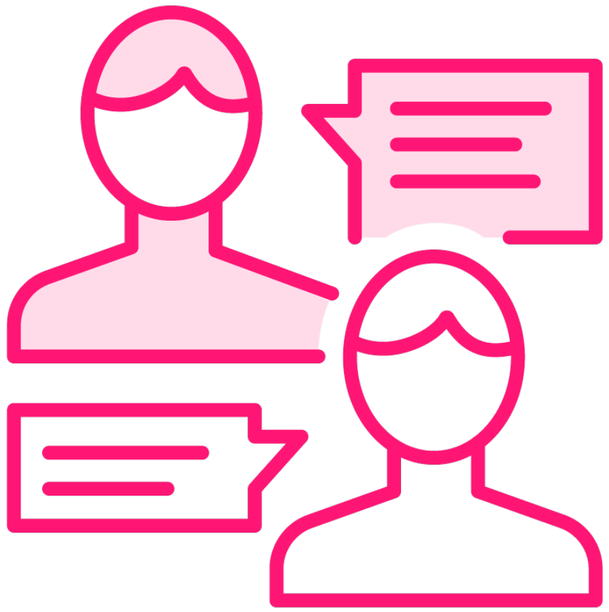
NIST SP 800-50

Awareness is not training. The purpose of an awareness presentation is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.

“What behavior do we want to reinforce.”

Awareness Requirements

Needs Assessment



Surveys

Interviews

- Management

Awareness course completion metrics

Analysis of events

- Ransomware
- Malware infections
- Phishing

Social Engineering

Manipulation of a person to do something they should not have done

Intimidation

Name dropping

Technical
e.g., Phishing

Appealing for help

Mitigating Social Engineering

Few technical controls available

The best control is awareness:

- Have a clear message
- Have an effective delivery method

Awareness of Social Engineering

How to recognize social engineering

What to do if exposed to an attack

What should a person do if they are a victim of an attack

Security Champions

Local staff to provide support for the development, implementation, and monitoring of the program

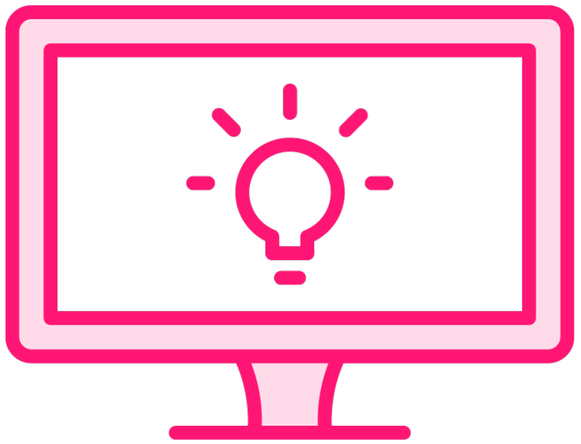
Key Points Review

Awareness is one of the most effective security controls available

Awareness programs should be based on the identification of needs

Awareness Program Deployment

Delivery of Awareness Programs



- Posters
- Screensavers
- Email
- Computer-based
- “brown bag”
- Awards
  - Games (gamification)
- Instructor-led sessions

Evaluation of Program

Surveys

- Evaluation forms
- Interviews
- Focus groups

Observation

Status reports

- Attendance

Indicators of Program Success

Sufficient funding

Management do not circumvent controls

Level of attendance

Content Reviews

Update of materials:

- New technologies
- New procedures
- New laws or regulations
- Change in culture
  - Ethics

NIST Special Publication 800-50

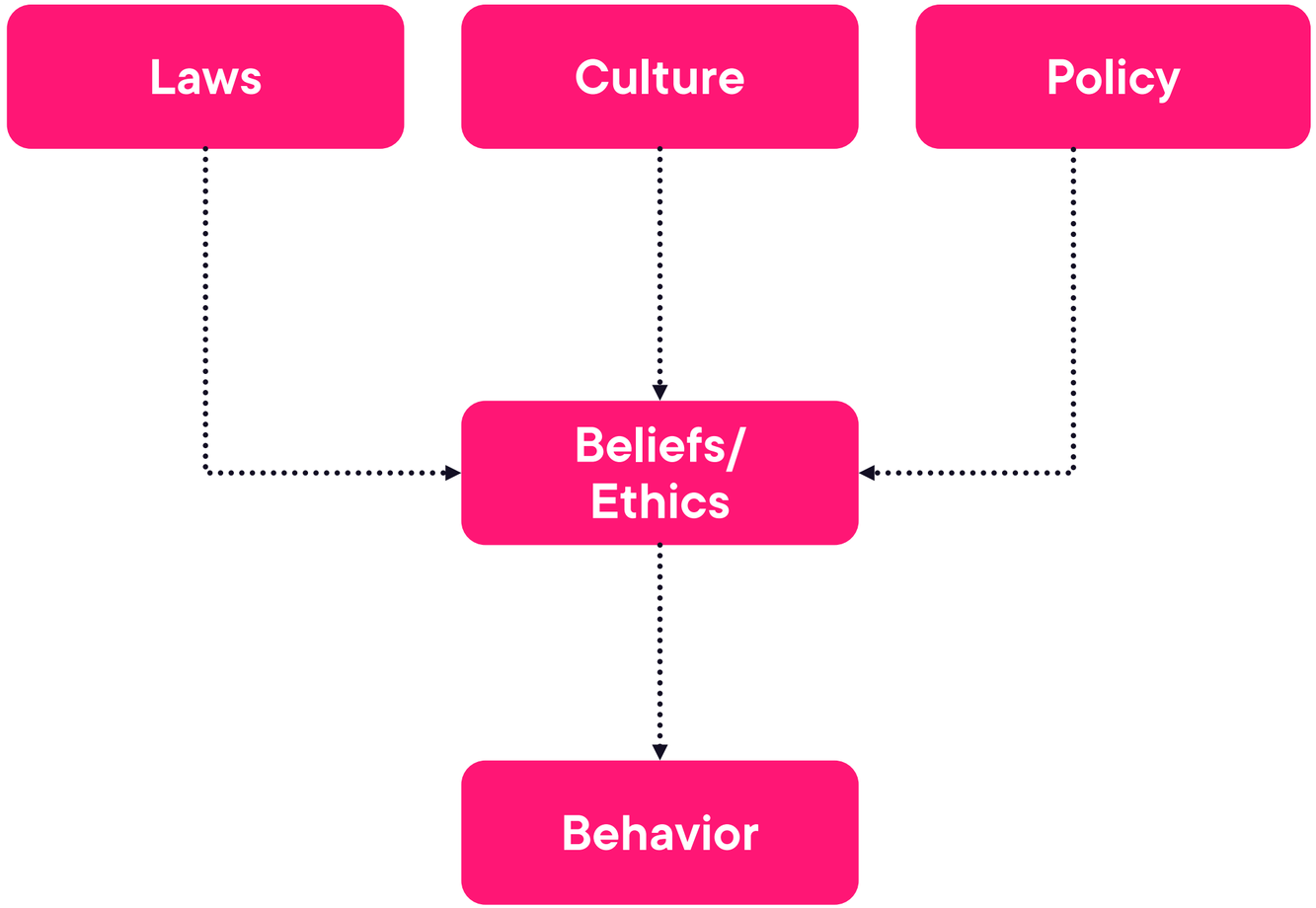
While improved security behavior can result in a decline in incidents or violations, reporting of potential incidents may increase because of enhanced vigilance among users.

Ethics

Ethics

Moral principles that govern a person's behavior or the conducting of an activity.

Oxford Languages



The core principle of ethics is:

“Do No Harm”

Ethics and Law

Ethics are not the same as law, although they may be based on law.

Professional Ethics

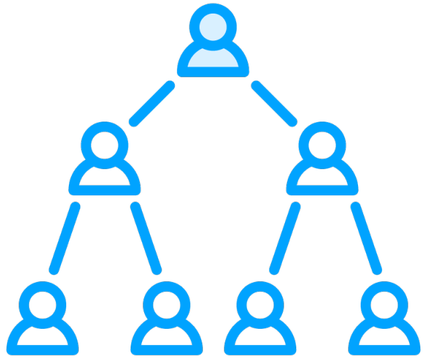
Membership in an organization

Standards of behavior and competence

- Continuous learning

Personal Versus Organizational Ethics

A person’s ethics may not be the same as the ethics of the organization



The development and communication of organizational ethics is required

Ethical Violations

Investigation

Suspension or termination of membership

Revocation of right to practice (Medical, legal, etc.)

Reputational damage

May also lead to criminal charges (Fraud)

Ethics Topics

May include:

Acquisitions and purchasing

Awarding of contracts

Insider trading

Behavior to employees or other personnel

Bullying, respect

Intelligence gathering

Competitor

Misuse of data for personal benefit

Key Points Review

Organizations should carefully develop a code of ethics that can prevent misunderstandings, provide direction and protect individuals and the organization from unethical practices

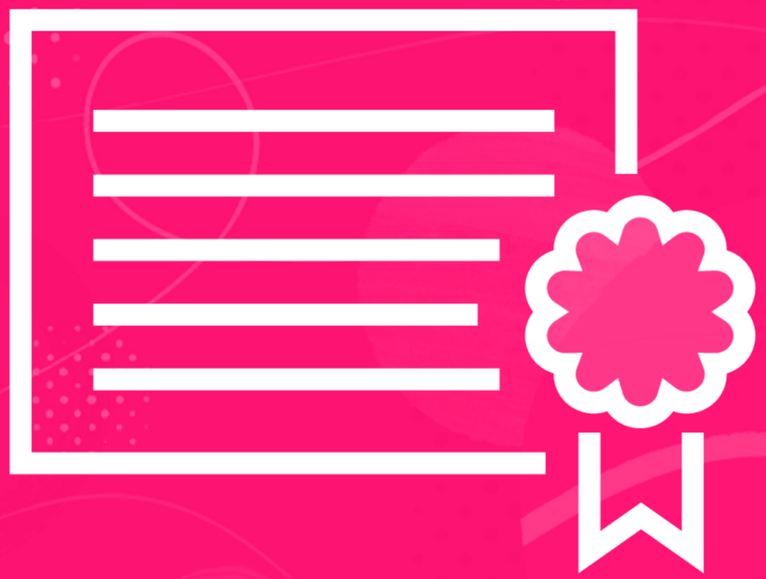
ISC2 Code of Ethics

ISC2 Code of Ethics

All information security professionals who are certified by ISC2 recognize that such certification is a privilege that must be both earned and maintained.

https://www.isc2.org/Ethics

Preamble

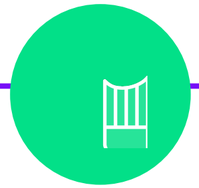


The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

https://www.isc2.org/Ethics

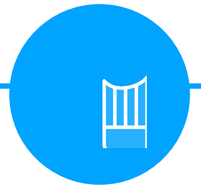
Code of Ethics Canons



Protect society, the common good, necessary public trust and confidence, and the infrastructure

Act honorably, honestly, justly, responsibly, and legally

Provide diligent and competent service to principals



Advance and protect the profession

Key Points Review

Ethics mandate acceptable forms of behavior

As Information Security practitioners we must follow, and encourage adherence to, good ethical practices