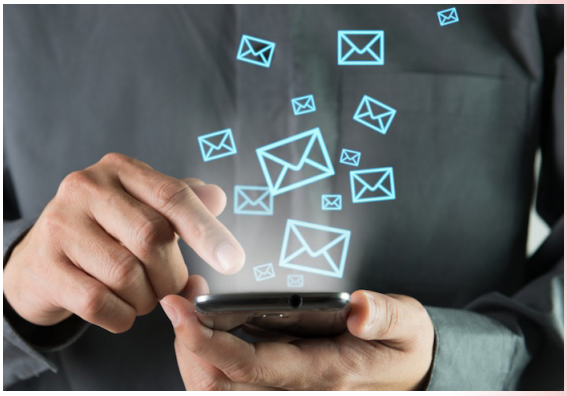
Symantec Security Awareness

The human factor is a major cause of security breaches

Keep your network safe by training your entire organization with Symantec Security Awareness web-based training. The modules can be integrated into your organization's learning system. We can even customize the training, and provide communications tools and other services to meet your company's security awareness needs and goals.

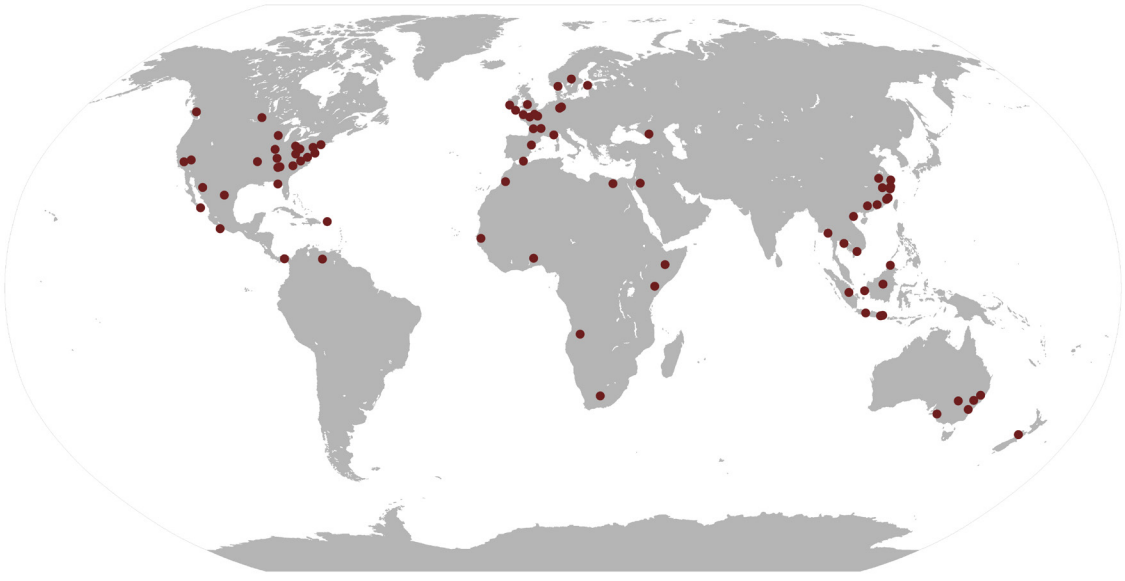


Your proprietary information is at risk every day and it's not just data that you lose. Data breaches cost money, customers, and even market share. Unfortunately, many breaches result from a lack of employee awareness of the security risks inherent in their actions.

Information security demands that employees practice proactive, security-conscious behavior. The **Symantec Security Awareness Program** trains your employees to understand information security issues and behave in a manner that minimizes risks—all in accordance with current regulatory requirements.

Company sample demo assessment

Assessment	Targets	Email Template	Training
500 targets	288 57.0% opened	184 36.0% clicked	93 18.0% exposed



1-866-NETXINC www.netxinc.com/training training@netxinc.com

Symantec Security Awareness Service
Module List and Descriptions

PCI AND HIPAA MODULES

Introduction to HIPAA
Language: English
Time: 6 min
Description: HIPAA governs the privacy of an individual's medical records. Training in HIPAA is mandatory for any employee that has access to patient data. All employees of an organization charged with maintaining HIPAA compliance need to know how to protect this data, and you can be held accountable for those records. This module does just that. It explains the what, how, and why behind HIPAA.

Introduction to PCI DSS
Language: English
Time: 6 min
Description: PCI DSS is an information security standard which was developed to increase and protect cardholder data during and after a financial transaction. It provides a global standard of technical and operational requirements, which ultimately results in a much more protected and happier consumer. This module is a high level explanation of what PCI DSS is, and how every employee is affected by it.

GENERAL SECURITY AWARENESS CORE MODULES

Passwords
Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 6 min
Description: Creating a complex password isn't hard – remembering it is. This module teaches efficient new methods of creating and remembering complex passwords required for your organization's security.

How Hackers Get In
Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 5 min
Description: It's not rocket science, anymore. Hackers can get in a variety of relatively easy ways – and most of those are through the user. This module reviews the different techniques used.

Human Firewall
Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 5 min
Description: Our modern networks contain a multitude of expensive filtering devices and software, but what about the human? This module outlines how users within your organization are a vital part of keeping your organization secure through filtering the information that enters and exits your network.

1-866-NETXINC www.netxinc.com/training training@netxinc.com

Privacy

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 6 min
Description: We all enjoy our privacy, and in our modern, digital world,privacy is especially important. This module teaches users what needs to be kept private and how to best protect that privacy.

Backups

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 6 min
Description: Do you have insurance on your house, car, or even your life? Backups for your information is like insurance for everything else – it doesn't seem necessary until something terrible happens. This module outlines what needs to be backed up and how to effectively do that, so that you aren't caught in a bind.

Data Protection and Destruction

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 5 min
Description: Every day we handle sensitive personal and organizational data that needs to be disposed of appropriately. This module outlines what data constitutes sensitive data and how to make sure it remains secure before and after you have used it.

Information on the Internet

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 5 min
Description: The Internet is an amazing tool that has given us access to an unprecedented amount of information, as such things that were once rare to know are now easily found on social media sites and web pages. This module teaches users how information on the Internet can be used against them and how to best protect themselves.

Staying Secure Online

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 6 min
Description: The Internet is an awesome resource; but without the necessary precautionary measures, it can be a real source of trouble. This module outlines how to securely use the Internet so that users can enjoy the resources without exposing themselves to the risks.

Phishing

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 6 min
Description: One of the biggest threats to an organization's security is the user that is susceptible to phishing attacks. This module teaches users how to identify different types of phishing attacks.

Appropriate Use

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 4 min
Description: Your users are consistently told which sites they cannot visit while at work, but many do not know why. This module outlines how those sites pose a threat to your company's security in order to eliminate a user's willingness to visit those sites while at work.

1-866-NETXINC **www.netxinc.com/training** **training@netxinc.com**

Insider Threats

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 5 min
Description: Most know that an organization can be attacked from outsiders like hackers and social engineers, but few understand that an organization can be attacked from the inside. This module outlines different ways an organization can be attacked from the inside, as well as how a user can be on the lookout and prevent these types of attacks.

Wi-Fi Security

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 6 min
Description: Wi-Fi connections are everywhere! Connecting to Wi-Fi at your favorite café provides convenience, but not without risk. This module teaches users what to watch out for when connecting to public Wi-Fi, as well as what to avoid doing while connected.

Working Remotely

Language: English, Chinese, French, German, Japanese, Portuguese, Spanish
Time: 5 min
Description: Working remotely has become more and more common leading social engineers to take advantage and hack sensitive information. This module illustrates different practices that should be avoided while working in public to ensure that you and your work are secure.

ROLE BASED TRAINING MODULES

Information Security Risk Management

Language: English
Time: 5 min
Description: Risk and business go hand in hand. Risk analyses and assessment is designed to fill in the variables for the risk equation for the organization. This module shows how to apply the risk equation to the organization to make sure that the security budget is being spent wisely. The module states that four threats or vulnerabilities are in the organization, identifies what the probability and impact those threats are, and analyzes the balance between threats and countermeasures.

Information Security Program Management

Language: English
Time: 4 min
Description: Failing to meet legislative security requirements costs companies big money, and the implementation of an information security program is the organization's defense against that potential loss. This module compares a well-run information security program to a factory, to be set up with a proper plan and well maintained throughout.

1-866-NETXINC www.netxinc.com/training training@netxinc.com

Laws and Legality

Language: English
Time: 5 min
Description: This module covers the protection of data, personal info, and more. It also covers the Privacy Act, HIPAA, E-Government Law of 2002, and FISMA. These laws mandate what security controls must be in place and followed in order to keep information safe and secure.

Organization Security Policies

Language: English
Time: 4 min
Description: When done right, the policies defined by the information security program determine what is valuable, who should have access to it, how it should be protected, what training is required for different levels of personnel, and what happens when a security issue arises.

System Policies

Language: English
Time: 5 min
Description: While federal and program-level policies help establish broad foundational standards, system-specific policies help to ensure the security of computers, networks, applications, and data.

Information Security Program for IT Security

Language: English
Time: 3 min
Description: This module focuses on the importance of all the different functions within the security organization.

Contractors

Language: English
Time: 4 min
Description: Contractors can be a great value to an organization. However, they can also introduce risk to an organization. Contractors are given access to secure data. When their contract expires, the threat of them leaving with that data must be avoided. This module explains the importance of screening, documentation, contracts, and more.

CIA Triad

Language: English
Time: 5 min
Description: Every security program revolves around CIA Triad-Confidentiality, Integrity, and Availability. This module explains the importance of remembering these three words, ensuring data and information is kept safe.

Information Security for Help Desk

Language: English
Time: 3 min
Description: The help desk is a crucial part of the information security program in most companies, and as such, should have an extensive understanding of security concepts as well.

IT Architecture Overview

Language: English
Time: 4 min
Description: IT Architecture can seem confusing. If you don't know your way around, it can seem a bit baffling. This module explains how to build an IT Architecture and demonstrates how all the parts work together to support one another, such as clouds, firewalls, and networks.

Securing Network Communications

Language: English
Time: 4 min
Description: Ensuring that sensitive information is kept safe and making sure that the information doesn't get into the wrong hands is critical. One example is segregating devices to protect the data that is being submitted. This module focuses on moving data in secure methods, such as encryption and more.

Network Security Controls

Language: English
Time: 5 min
Description: What measures are put in place to ensure that hackers can't get in to do damage? This module focuses on network access control to allow only those who are authorized to connect their host to the network. It also focuses on segregating network zones and protecting against low-level network attacks and traffic interception, along with alerts to any threats that may exist.

Information Security Risk Basics

Language: English
Time: 4 min
Description: In information security, we define risk by Ira Winkler's risk equation: Threats multiplied by vulnerability, divided by controls or countermeasures, all multiplied by what's at stake. A threat is anything that can harm you or your system. A vulnerability is anything that is considered a weakness in the system. Ccontrols are something that mitigate or deal with threats or vulnerabilities.

System and Data Ownership

Language: English
Time: 4 min
Description: While IT is in charge of the organization's infrastructure, they can't be entirely responsible for the data on the systems. This module explains the divide between the IT Department and the business process owners of the data (finance).

Information Security Specific Roles

Language: English
Time: 11 min
Description: This module explains the importance of each role within an IT department. The module uses the "factory" metaphor again. Each part of the machine, or factory, must work efficiently in order for the entire process to run smoothly.

Human Resources Security

Language: English
Time: 4 min
Description: Proper personnel security is of upmost importance. The policies and practices implemented should reduce the risk of theft, fraud, or misuse of information by employees, contractors, and third-party users.

Remote Access

Language: English
Time: 4 min
Description: With the changing working environment and the addition of remote work environments, we are now able to access work resources from coffee shops, home, or even airplanes. This module explains the importance of security of VPN's, USB's, and more. Some of the remote access solutions in the module include limiting the resources that are provided to remote users and strongly enforcing the use of secure authentication mechanisms.

Security in the System Development Lifecycle

Language: English
Time: 4 min
Description: Each technology that an organization deploys goes through distinct phases of its deployment. Because of this lifecycle, information security controls need to be integrated at each step to ensure that risk is minimized and each technology runs smoothly. This module focuses on the different steps to make sure this happens.

Operation Security

Language: English
Time: 14 min
Description: Even though Information Security did their job making sure that the system was secure when it was deployed, the hackers in the world never give up. Information Security needs to take into account how the day-to-day operational activities of this security organization will change to account for a new solution.

The Certification and Accreditation Process

Language: English
Time: 4 min
Description: Because of regulations, federal agencies are required to prove that they're doing their jobs protecting information under their control and on their IT Systems. This module explains the process and how this process is designed.

Contracting and System Acquisition

Language: English
Time: 3 min
Description: At some point, every business will have to deal with outside vendors and contractors. And in working with these vendors, many things regarding security can go wrong. This module explains the risks in the contracting process that should be taken seriously.

Physical Security

Language: English
Time: 12 min
Description: This module explains the importance of physical security and keeping the information within your organization safe from a physical standpoint. It focuses on details such as door locks and access cards, making sure that only those who are granted access to a certain location can access it.

Media Handling

Language: English
Time: 4 min
Description: A critical component of your organization's security is how your employees handle the data that they are entrusted with. This means they have to manage how they ship, store, destroy, label, and back up media that they use for work purposes.

Contingency Planning and Disaster Recovery

Language: English
Time: 5 min
Description: Let's face it, things will go wrong within an organization. But how you plan for the disaster is the difference maker. With a proper plan for the disaster that you face, it can be responded to effectively, and it can be minimized.

User Security

Language: English
Time: 4 min
Description: In security, we talk about threats to our users all the time. Yet every organization spends time, money, and resources on security awareness training. The most important thing to remember is that awareness training is two separate acts. The first goal of what we call "awareness training" is literacy. We put users through this training so they have a common vocabulary about information security. The second step in creating a security-aware user is behavior design. Changing user behavior is often taken for granted.

Improving Information Security Performance through Education

Language: English
Time: 5 min
Description: The constant evolution and change within the threat landscape causes the entire industry to constantly change the education landscape. We need to re-engineer security education on a regular basis.

Access Control Basis

Language: English
Time: 4 min
Description: Access Control is a collection of methods and components used to protect information assets. It is used to control the confidentiality and integrity of a secure system. It ensures that certain information is available only to those authorized, and those who are not authorized, cannot modify secure information.

Incident Response Basics

Language: English
Time: 5 min
Description: While systems are designed to prevent issues from happening, no security control system is 100% effective against attacks. When this happens, a fast and well-practiced response is what allows an organization to limit losses from an incident. The most important factor in quickly responding to successful attacks is to have a well-prepared Computer Security Incident Response Team (CSIRT).

Information Security Program for IT Department

Language: English
Time: 4 min
Description: The IT department is in many cases the first responders to a security incident. Because of this, it is a critical piece of the overall Information Security puzzle. IT and InfoSec need to work together as a single unit in order to provide the more secure environment.

Vulnerabilities, Threats, and Controls

Language: English
Time: 4 min
Description: When creating an effective IT system, all of the relevant vulnerabilities, threats, and their control measures must be actively observed and considered in order to present the most efficient and secure solution.

Audit and Assessment

Language: English
Time: 3 min
Description: The purpose of the Audit and Assessment business unit is to provide an objective, external set of eyes – as a third party – to ensure any IT solution is truly as secure and effective as possible. This module covers those aspects and explains how Audit and Assessment fits into the overall InfoSec posture.

About NetX Information Systems

Trust • Value • Partnership

Established in 1997, we remain a leader in customer service and an innovator in approaching the challenges IT Departments are faced with today. Our philosophy is to establish trust, add value and maintain a long term partnership with our customers and vendors.

Our dedication to a single vendor in each technology area allows us to focus on being subject matter experts in the products we recommend to our customers.

Data Protection • High Availabilty • Endpoint Management
Archiving • eDiscovery • Security

1-866-NETXINC **www.netxinc.com/training** **training@netxinc.com**