SECURITY COMPASS WHITEPAPER

Mapping Security Awareness Training to Regulatory Requirements

Security Compass

Software security training programs help build a culture of security in your organization as well as raise awareness among employees. It's also a requirement under many regulatory standards and laws.

Most organizations have policies, processes, and tools to manage external threats, however internal actors play a major role in data breaches. In a McAfee study, it was found that internal actors contribute to 43 percent of the data breaches from which 22 percent are accidental.

To adequately address the accidental losses from internal people, organizations should focus their attention on security training. An investment in training to improve your security posture not only helps you to develop secure products but also saves a lot of time spent on remediation activities.

Though security professionals are responsible for integrating security into systems and processes, the ever-rising threat landscape makes it difficult for them to cover all applications and people. Especially in a fast-moving DevOps environment, it's manually impossible to secure every application. That's why it would be ideal if everyone involved in the software development process acquires a basic understanding of security practices.

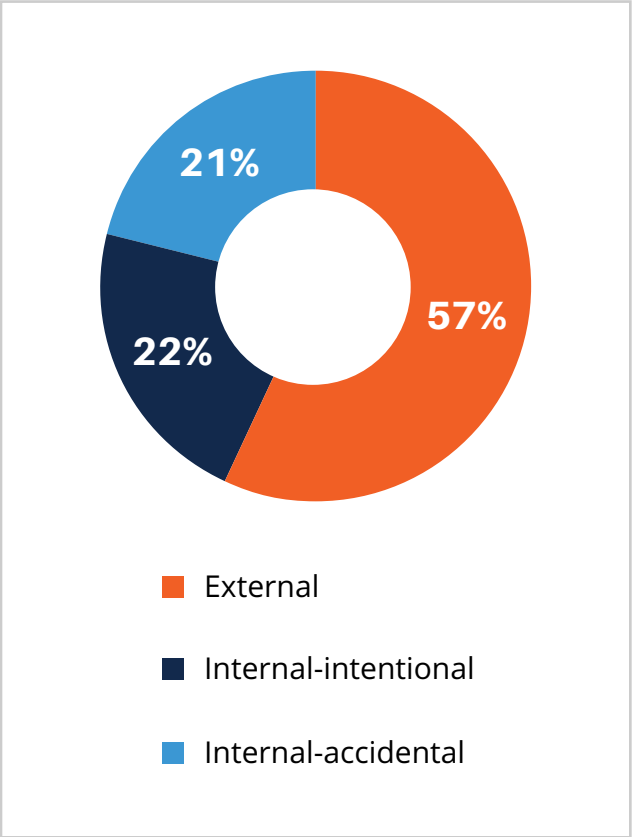


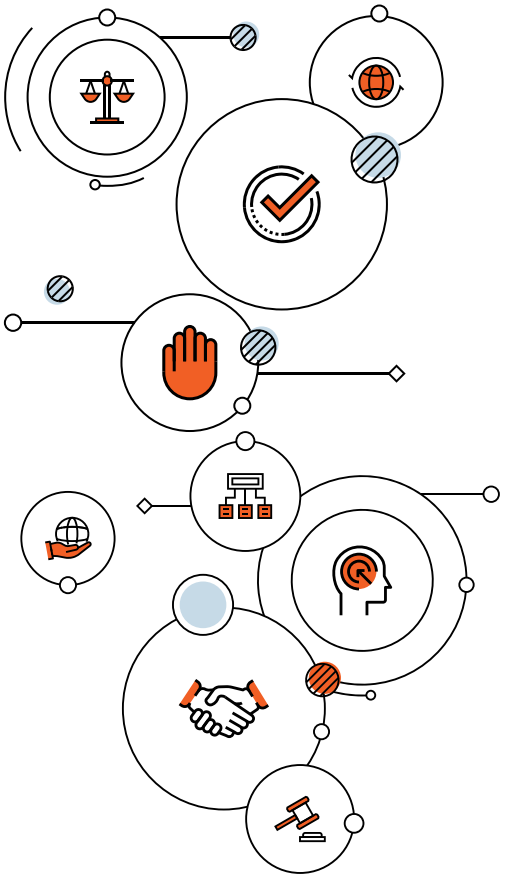
Figure 1. Actors involved in data breaches.

Software security training enables DevOps teams to develop secure code and saves the efforts wasted in patching vulnerabilities.

Compliance requirements for security awareness training

Many regulatory standards and laws mandate organizations to ensure employee security awareness training for compliance. With a rise in data breaches and the unintentional involvement of employees in those cyberattacks, it's no wonder that regulatory bodies are emphasizing the need to train employees.

We're making a list of standards and laws that require organizations to implement a security awareness program for employees.



General Data Protection Regulation (GDPR)

Since the EU implemented the GDPR for data privacy and protection, organizations are making efforts to comply with these regulations as non-compliance can lead to huge penalties (of up to 4 percent of global annual turnover). GDPR states the need for employee training under multiple sections.

- In Article 39 where the tasks of the data protection officer are listed, the law states that the officer has to monitor compliance with raising awareness and training employees. Though this talks about compliance with training, it's important to note that the lawmakers expect organizations to impart training.

- In Article 47, the GDPR clearly requires organizations to impart "the appropriate data protection training to personnel having permanent or regular access to personal data."

The GDPR doesn't specify what training should entail but keeping your employees updated with the latest privacy awareness training for GDPR can help you to protect customer data.

Health Insurance Portability & Accountability Act (HIPAA)

The HIPAA law is applicable to all organizations and their partners involved in the healthcare sector. Even if your organization isn't involved in healthcare but stores patient information, you're bound by the regulation.

HIPAA requires organizations to implement a training program for security awareness and training for all employees handling personal health information (PHI).

The HIPAA Privacy Rule specifically mentions the security training requirement for new employees. Basically anyone who joins an organization, that is bound by HIPAA, has to be provided security and privacy awareness training within a reasonable period. It also states the need for training all employees if there's any material change in policies and procedures.

Payment Card Industry Data Security Standard (PCI-DSS)

The PCI-DSS standard was developed to protect consumer information in financial transactions and is applicable to all organizations handling branded credit cards.

- The security awareness requirement for this standard requires education for all employees on the importance of protecting credit cardholder information
- The standard also specifically focuses on training developers at least once a year to educate them about common coding vulnerabilities and secure coding practices.

California Consumer Privacy Act (CCPA)

The CCPA, signed into law in 2018, intends to enhance data protection and privacy rights for the residents of California, U.S. The requirement to train employees is stated in this law for everyone handling consumer inquiries about their organization's privacy practices.

Employees should be trained on the rights of consumers in California with respect to their privacy under the statute and how they can exercise these rights.

NIST 800-53 (new Revision 5 standard)

The National Institute of Standards and Technology (NIST) published its long awaited Revision 5 of the NIST 800-53 Standard in September 2020. The updated standard includes a catalog of privacy and security controls to support the security of U.S. federal information systems. NIST 800-53 includes an entire control family for security awareness training.

The Awareness and Training Control family under NIST 800-53 Revision 5 includes the following controls:

No.	Control
AT-1	**Security awareness and training policy and procedures** The organization should develop and disseminate a security awareness and training policy as well as review and update it periodically.
AT-2	**Literacy training and awareness** The organization should provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. This includes security awareness training to all information system users as part of their initial training; when changes in information systems warrant training; and thereafter.
AT-3	**Role-based security training** The organization should provide security training to employees responsible for performing security activities before allowing access to information systems; when changes in information systems warrant training; and thereafter.
AT-4	**Security training records** The organization should document and monitor security training activities for each information system; including basic awareness training and specific system training. They should also retain the record of training for a certain time period as defined by the organization.

NIST 800-171 that was published to protect Controlled Unclassified Information (CUI) in non-federal information systems also includes similar security awareness training controls.

Under the awareness and training requirements, organizations are required to:

- Ensure all users of organizational systems are made aware of the security risks of their activities. They should also be trained on all security policies, standards, and procedures related to those systems.
- Ensure that all employees are appropriately trained to carry out any information security tasks.
- Train employees to identify and report any indicators of insider threat.

Application Security and Development Security Technical Implementation Guide (STIG)

This guide was published to ensure the security of information systems for the U.S. Department of Defense; and these requirements were borrowed from the NIST 800-53 and other documents.

When it comes to training, the document highlights the need for annual security training for all levels of program management, testers, developers, and designers related to their job function.

Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification, released in January 2020, is a compliance standard designed by the U.S. Department of Defense to protect sensitive information across the Defense Industrial Base (DIB). This new standard was published to ensure security of data located on the information system of contractors.

CMMC also has a complete domain dedicated to awareness and training. Apart from similar training requirements as laid out in NIST 800-171, this new model also has the following controls:

- Contractors should provide awareness training to help employees recognize and react to threats from suspicious behaviors, breaches, advanced threat actors, and social engineering. The training material should also be updated at least annually or whenever there are any changes to the threat landscape.
- The training program should include practical exercises wherein the scenarios are related to current threats. Feedback should be provided to those participating in the training.

Because of the increasingly sophisticated threat landscape, the U.S. Federal Government intends to ensure information security by mandating training on the latest threats.

What is an effective security training program?

Any training, no matter how important, loses its value if the training material isn't designed keeping the audience persona in mind.

When it comes to training your DevOps teams who are already burdened with tight delivery deadlines, you should consider the challenges they face with security best practices. They might be aware of standards for data protection, but the right training can help them write secure code.

Moreover, you have to ask them the right questions to get buy-in for security awareness training. For instance, would they prefer building secure code in one attempt through training or work endlessly on patching vulnerabilities?

The key to an effective program is delivering the relevant information to the right audience at a time when they're inclined to consume that information.

Security awareness training is a strategic advantage

Introducing a security training program early can change the way employees see privacy and security compliance. While GDPR grabbed the attention of everyone around the world because of its comprehensive privacy laws, more and more countries, industries, and regulatory bodies are expected to follow suit. Considering the rising number of data breaches, privacy is one of the major concerns among the public these days.

Though product security is the end goal for most organizations when it comes to security awareness training, what you shouldn't underestimate is the impact being proactive has on your customers. Most organizations have the tools and processes to build security into software, but not many make the effort to build a culture around security. Only when your employees buy into the idea of security, you can make strategic leaps to position yourself as a responsible organization.

If you're looking to comply with these training requirements or need help with designing a security awareness training program, please get in touch with us.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
995 Market Street
2nd Floor
San Francisco, CA
USA 94103

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001