Learning 2018

Cybersecurity | The New L&D Frontier

DISCLAIMER

The guidance provided in this presentation was prepared exclusively for the benefit and internal use of the party to whom it is delivered (each, a “Recipient”). The guidance is not intended as, nor shall be deemed to constitute or contain, advice on which the Recipient may rely and is confidential and proprietary to JPMorgan Chase. The guidance may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. This guidance is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The Recipient is responsible for determining how to best protect itself against cyber threats and for selecting the cybersecurity best practices that are most appropriate to its needs. JPMorgan Chase assumes no responsibility or liability whatsoever to any person in respect of such matters, and nothing within this guidance shall amend or override the terms and conditions in the agreement(s) between JPMorgan Chase and the Recipient.

Awareness Components
Overview
Annual Compliance Training
Marketing & Comms
Phishing & Social Engineering
Other Awareness Support
Education Components
Define Audience(s)
Role-based learning
Certifications
Skills Management
Learning portals
Training Providers

Cyber Awareness Program Overview

Overview

Critical components of a Cyber Awareness Program:

- Annual Compliance Training
- Marketing
    - Web Portal
    - Video Series
    - Articles
    - Events
    - Communications
- Ambassador Program
- Social Engineering Program
- Future: Short Gamified Assessment

Annual Compliance Training

No one wants to be the next company in the news for a cybersecurity breach. Whether mandated by your CEO, Board of Directors, Regulators, or just good common sense, it is important to have a formal component with an audit trail. We have found an annual training module to be a valuable and effective way to ensure that the critical best practices are being communicated to each employee. This is also a foundational component if your team is hoping to launch a social engineering program.

Marketing

Video Series

- Cost - Low
- Maintenance - Medium
- Potential Vendors
    - Twist & Shout – Restricted Intelligence (http://www.restrictedintelligence.co.uk/)
    - Habitu8 (https://www.habitu8.io/)
- Video series may be episodic and run on a recurring schedule, or modular and be used adhoc based on business needs and priorities.
- Several vendors provide sample communications and marketing materials in addition to the video content. Campaign materials may include banners, email templated, takeaway pdfs, and more.

Web Portal

- Cost – Medium
- Maintenance – Medium
- Publishing via a webpage is often a great tool for disseminating information. Webpages are perpetually available and accessible. In addition, webpages can make searching for specific information less cumbersome than a traditional elearning module. Consider making the investment to build a user-friendly and attractive web presence.

Events

- Cost – Low to High
- Maintenance – High
- Event-focused awareness offers the opportunity to reach people at scale but comes with a set of challenges. Budget and human resource constraints could impact those with sizeable geographic scope. For those whose employees sit in a handful of centralized locations, events can be a more effective use of investment and time. Possible event types of may include Video Binge Events, Lobby Exhibits, Panel Discussions, Keynote speakers, etc.

Articles & Communications

- Cost – Low
- Maintenance – Low to High
- Publishing articles via your company homepage, newsletter and/or blog space is another channel to consider when spreading the word about cybersecurity. To avoid the high time investment of writing a new article each month, consider republishing a ready-to-go article from one of the public resources below.
- Potential Resources
    - DarkReading https://www.darkreading.com/
    - Krebs on Security https://krebsonsecurity.com/
    - Schneier on Security https://www.schneier.com/
    - US-Cert https://www.us-cert.gov/ccubedvp/past-blogs-and-articles
    - SANS Internet Storm Center https://isc.sans.edu/
    - SANS Ouch Newsletter https://www.sans.org/security-awareness-training/ouch-newsletter

Ambassador Program

Setting up an ambassador program is another consideration when establishing a cyber awareness program. This may be particularly helpful when your organization is spread out geographically and/or where there are multiple independent business silos. The goal of every ambassador program is simple: centralize the design, messaging and development of materials, and then decentralize the dissemination of the product.

Social Engineering Program

Phishing is one of the most common ways for cyber threats to enter an organization. This is because they are cheap to build/deploy and are surprisingly effective. If you are curious where to start on your cyber awareness journey, phishing is undoubtedly that point. Fortunately, there are numerous providers that are tackling this issue. Phishing, unlike some other topics, is about muscle memory. The issue is not that it is complex, but that it is counter-intuitive to our daily routine. We see an email, we click an email. We are not trained to be suspicious of our inbox. However, that is exactly the behavior and mentality we hope to instill in our colleagues. Hackers thrive with phishing not because of our logic, but because our emotions such as fear, greed, and curiosity. Through simulated phishing attempts, employees are taught to identify when these red flags are triggered. Some potential vendors in the phishing and social engineering simulation space include:

- Phishline https://www.phishline.com/
- Cofense (formerly PhishMe) https://cofense.com/

Cyber Education Program Overview

Overview

Critical components of a Cyber Education Program:

- Define Audience(s)
- Role-based learning
- Certifications
- Skills Management
- Learning portals
- Training Providers

Define Audience(s)

Per standard learning requirements procedures, first identify who your intended audience will be. Cybersecurity is a broad subject area that is enabled by cyber professionals, technologists (software engineers, system architects, etc), audit and controls specialists, program management support and many more skillsets. Define your target audience early to avoid confusion and overlap with other potential programs.

Role-based Learning

Role-based learning is a critical component of any learning program. It often can demonstrate progression and may improve retention.

Certifications

Where appropriate and desired, consider utilizing external certifications to demonstrate capability for specific roles. We've identified several popular certifications related to various roles throughout the cyber arena.

Role	Popular Certifications
Cyber Operations	• GIAC Certifications (SANS) • CEH
Penetration Testing	• OSCP • OSCE
Cyber Program Management	• CISSP • Security+
Cyber Audit / Controls	• CRISC • CISA • CISM
Tech / Cloud	• CCSP

Skills Management

Technology-based roles like cybersecurity require more detailed ways of tracking the knowledge, skills and abilities of the individual. Tracking progression and proficiency at the skill level enables organizations to more quickly identify in-house talent, mobility opportunities and gaps. Ideally skills would be updated and refined based on business needs at the role level. A skills management portal / program is a vital component for the future of tech learning.

Learning Portals

Consider launching a web portal for your cyber professionals. Providing a unified experience for technologists is critically important especially if you hope for your materials to be seen and used. Presenting a user-friendly experience saves technologists time and helps them find critical information more effectively, ultimately aiding in the better defense of the organization.

External Training Providers

Due to the rapidly changing nature of technology and the cybersecurity landscape, it may be difficult to develop and maintain adequate expertise internally. You might consider relying on external content providers and SMEs to aid in your ability to train your cyber professionals on the latest tech, tactics and procedures.

Vendor	Certifications
National Initiative for Cyber Education (NICE) (free)	• The NICE Framework, is a focused resource that categorizes and describes cybersecurity work. The NICE Framework, establishes a taxonomy that describes cybersecurity roles.
Cybrary.IT (free)	• Discover the possibilities. Learn anytime, anywhere with open-source, high quality training from subject matter experts, industry professionals, and thought-leading companies.
Cyber Aces (SANS) (free)	• SANS Cyber Aces Online makes available, free and online, selected courses from the professional development curriculum offered by The SANS Institute, the global leader in cyber security training.
SANS ($$)	• SANS is the most trusted and by far the largest source for information security training and security certification in the world.
InfoSec ($$)	• InfoSec Institute was founded in 1998 by an expert team of information security instructors. Their goal was to build a business by offering the best possible training experience for students.
ISACA ($$)	• ISACA® is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance.