CYBERBIT
PROTECTING A NEW DIMENSION

Enterprise Cyber Awareness and Simulation Training Guide

White Paper

www.cyberbit.com | sales@cyberbit.com

Table Of Contents

Introduction

The people, not just tools, are the key to enterprise cyber security. It's time to devise an actionable plan to make sure every member of your organization is cyber-ready. In this guide, we will present a basic framework for optimizing the types, frequency and costs of security simulation training for the entire enterprise.

The Need for Simulation Training

Simulation is an essential training technique for high-risk, high-pressure fields. The first flight simulator was established in 1910 and was further developed in WW1 and WW2, as aircraft became more complex to handle. Simulation has been popular In the medical community as early as 1967 with Sim-One - the first computer controlled patient simulator. Simulation training is used in fields where the cost of error is high, fast response is critical, and the environment is complex. Practicing complex scenarios such as surgery, or an aircraft malfunction, in advance substantially increases the trainee's performance during a real-life situation, and reduces risk.

Organizations are facing similar risks when it comes to cyberattacks. With threats being more complex and attackers more sophisticated, there aren't enough skilled defenders to match the adversaries. Though expensive new security tools are released each month, these acquisitions haven't improved outcomes.

An organizational awareness and training program is designed to ensure that all employees have the skills and experience they need to respond correctly in the face of cyber emergency. Since most traditional training methods have been coming up short, companies are finally beginning to take heed. In a recent survey, The Enterprise Strategy Group (ESG) and ISSA found that 39% of cybersecurity professionals recommended increasing cyber security training for nontechnical employees. Clearly - cybersecurity leaders are concerned that every member of the organization have proper security training and are shifting their investment priorities to reflect this.

A cost effective investment

Moreover, while traditionally it has been been difficult for businesses to prove return on investment for security tools and systems, simulation training delivers easily quantifiable results. It's clear to see how much you're saving by reducing hires and to estimate the cost savings associated with improving cyber security KPIs such as TTD (time to detect) and TTR (time to respond). This makes simulation training a cost effective strategy.

In this guide, we will present the basic guidelines for optimizing the types, frequency and costs of security simulation training for the entire enterprise.

Enterprise Cybersecurity Simulation Training

Executive Leadership
- Cyber Crisis Response

CISO & SOC Manager
- Cyber Crisis Management
- Attack Simulations

Senior Management
- Cyber Incident Response
- Tabletop Exercises

Tier 1 Security Analysts
- Incident Response - Triage, Investigation & Response

IT Department
- Coordinated Cyber Response Drills

External Contractors
- Cyber Security Awareness & Prevention

Tier 2 & 3 Security Analysts
- Advanced Investigation & Response
- Skill Workshops

General Employees
- Cyber Security Awareness & Prevention

CYBERBIT
PROTECTING A NEW DIMENSION

1. Executive Leadership

CEO, CFO, Sales & Marketing, Communications

WHO: Executive Leadership

WHAT: Cyber Crisis Response

Background:

Current Corporate Policies / Standards
Generating Corporate Cyber Goals / Objectives
Developing Corporate Response Policies and Standards
Roles Key Cyber Staff
Personal Responsibility for Actions
Compromise Consequences / Business Impact
Threats / Entry level
Detection / Mitigation – Entry Level

Cyber Skill Level: Medium

Duration: 1-3 hours

Frequency: 1x per year

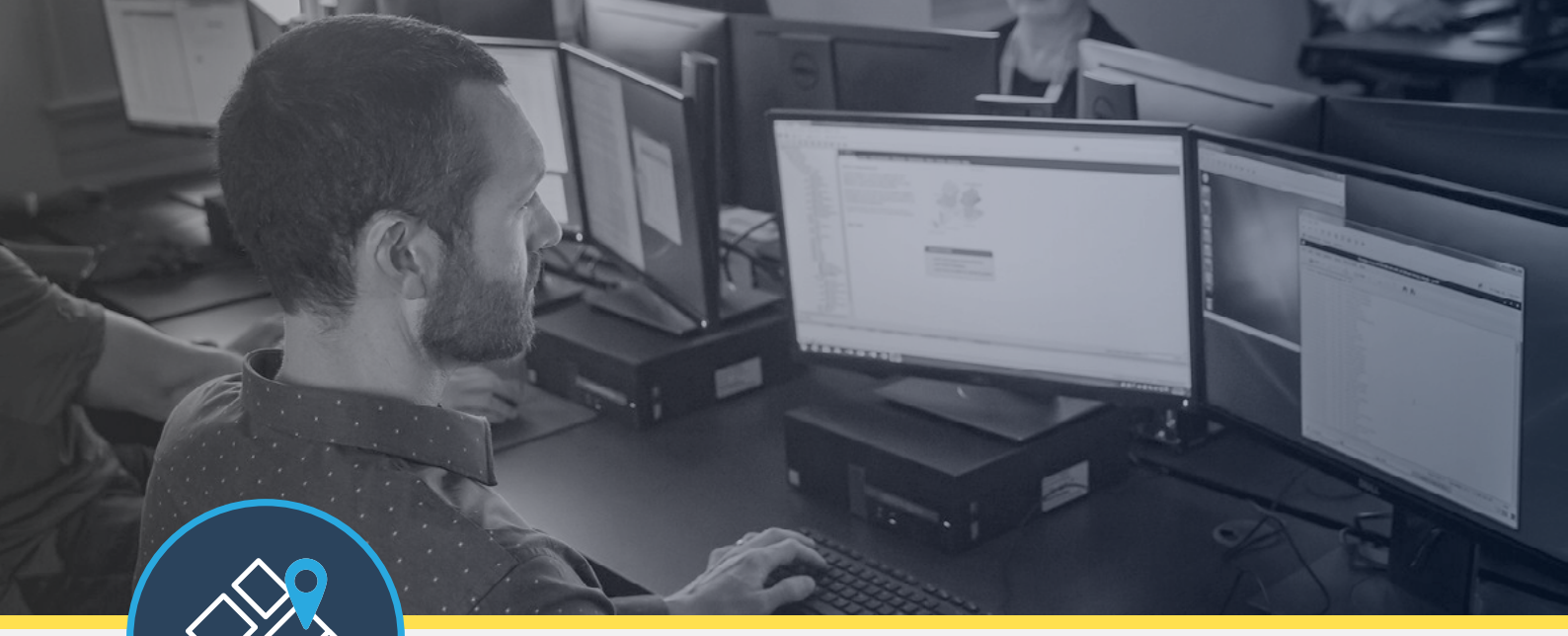
Cost: $5,000 (5 executives)

Cyber Skill Level: Medium

Responsibilities: As the top decisions makers, executive managers take an active and important role in the execution of all policies. Therefore they need to be aware and informed, regarding the overall organizational security posture - from the tools, staffing and the contingency plans to the rationale behind security strategy. And when there is a crisis, this is the group who will be responsible for deciding how to respond. For example, the communications leader must decide if and when to make public statements regarding a breach.

Challenges: There is often a tendency among executive leaders to underestimate the importance of security. Therefore, keeping them engaged and invested in security initiatives may take significant efforts.

Training: Give executives hands-on practice responding to a full blown Cyber Crisis. In this training and simulation module, executives get an opportunity to practice in a fully realistic simulated environment. Possible situations range from: ransomware scenarios where they must decide whether or not to pay the ransom, creating and approving public statements regarding breaches, sharing breach information with law enforcement agencies, etc. All so that when incidents do arise, executive management is equipped with the necessary skills to respond fast and effectively to emergent situations.



2. Senior Management

WHO: Senior Management

WHAT: Cyber Incident Response Tabletop Exercise

Background:
Corporate Cyber Team / Responsibilities
Generating Corporate Policies and Standards
Current Corporate Policies / Standards
Personal Responsibility for Actions
Compromise Consequences / Business Impact
Threats / Entry level - Basic
Detection / Mitigation - Basic
Response Basics

Cyber Skill Level: Low

Duration: 4 hours

Frequency: Once per year

Cost: $5,000.00 + expenses (10 managers)

Responsibilities: While not directly involved in managing cybersecurity incidents, senior managers often play an important role in decision-making during high profile breaches and ransomware attacks. Each department manager must understand the security posture and risks of their departmental assets and quantify the cyber risk they pose to operations. For example, department managers must be aware of problems or vulnerabilities with ERP and other software platforms. Further, a business unit director must understand if paying a ransomware fee is the right move in certain situations because the lack of service might have a far more devastating business impact than simply paying the fee. Additionally, they are responsible for setting access and authorization levels to departmental resources and enforcing procedures.

Challenges: Senior managers need to understand the risks of strategic departmental assets and determine and enforce cyber security procedures. During major breaches, they must be be kept informed, take an active role in response, and be a part of critical decision making in real-time.

Training: Quarterly breach response drills train senior managers and business owners by simulating cyberattacks that are relevant to them. Each session lasts approximately 4 hours depending on need and sessions can be tailored to fit the exact departmental needs.

Sessions will provide the tools to: simulate effective breach notifications, assess business impact, make business decisions regarding services shutdown/runtime in crisis time and making sure the business is affected as little as possible. Possible scenarios can cover ransomware, to major data leaks, to DDoS attacks, to phishing and spam attacks. All aspects are targeted in a participatory way to give this group the tools they need to successfully lead their departments during a cybersecurity breach.

3. CISO and SOC Manager

WHO: CISO & SOC Manager

WHAT:
Cyber Crisis Management & Attack Scenarios

Background:
Current Corporate Policies / Standards
Enforcing Policies and Standards
Personal Responsibility for Actions
Review Threats - Expert
Review Detection / Mitigation - Expert
Responses
Range Simulation / Interaction / Review (3 Scenarios)

Cyber Skill Level: High

Duration: 2 full days

Frequency: 2x per year

Cost: On Site (Group of 5) $16,000.00 + Expenses

Cyber Skill Level: High

Responsibilities: The CISO and/or SOC Manager are responsible for cyber security of the organization, bottom line. In the event of a breach, the CISO/SOC Manager must be abreast of all developing information in real-time and use it to make critical decisions, all while maintaining timely, accurate communications with the organization and outside entities such as the press, law enforcement and key allies in the cybersecurity community.

Challenges: The CISO/SOC manager position requires facing many challenges such as managing multi-tier response teams, ensuring preparedness and prevention, aligning security efforts with business goals and handling cyber crises, from beginning to end. The responsibility of security lies squarely on the shoulders of the CISP or SOC manager. Thus you must do all you can to ensure that in the face of emergency, everyone knows their roles and responsibilities and performs them perfectly.

Training: Fully simulated cybersecurity training and practice will prepare CISOs and SOC managers to respond flawlessly when a cyber breach begins. Having practiced for the inevitable over and over, CISOs and SOC managers are better equipped to react optimally, despite the great pressure and intensity of the situation at hand. Simulation training also yields critical insights into organizational and procedural weaknesses and allows time to address them before the real crisis begins. The CISO and SOC manager should also run attack-scenario specific drills for all of the most pertinent cyber attack types: Ransomware, DDoS, Data & Privacy Leak, and more.

4. Tier 1 Security Analysts

WHO: Tier 1 Security Analysts

WHAT:
Incident Response - Triage, Investigation & Response

Background:
Current Corporate Policies / Standards
Enforcing Policies and Standards
Personal Responsibility for Actions
Review Threats / Entry level - Expert
Review Detection / Mitigation - Expert
SIEM Review
Incidence Response
Range Simulation / Interaction / Review (3 Scenarios)

Cyber Skill Level: Medium to High

Duration: 2 full days

Frequency: 2x per year

Cost: On Site (Group of 5) $16,000.00 + Expenses

Responsibilities: Your Tier 1 Analysts are the first responders for all incoming security alerts. They are your organization's first line of defense. The better they do their job, the less the stress is put on everyone else. The Tier 1 analysts monitor and triage alerts, identifying high risk situations and make the decision to escalate events when necessary. They also perform preliminary incident investigations.

Challenges: The threat landscape is constantly changing and these relatively less-qualified analysts often lack the experience in crisis and breach management. Their lack of knowledge and experience means they tend to escalate too many alerts, creating a burdensome backlog for the Tier 2 analysts. When Tier 2 analysts are overloaded with alerts, they have trouble dedicating their efforts to the most critical and difficult incidents. They also have difficulty mastering the large number of security tools they are expected to know how to use. Additionally, Tier 1 analysts suffer from 'alert fatigue', resulting from the overwhelming amount of alerts generated by all the SOC tools.

Training: Simulation training, modeled after the events they deal with on a daily basis, as well as emergency situations, helps prepare Tier 1 analysts to react more efficiently and effectively in their daily work as well as emergent situations. Simulation training allows relatively new, inexperienced analysts to gain practical experience quickly, allowing them to build confidence and advance their skill level more quickly.

5. Tier 2 & 3 Security Analysts

WHO: Tier 2 & 3 Security Analysts

WHAT:
Advanced Investigation & Response, Skill Workshops

Background:
Current Corporate Policies / Standards
Enforcing Policies and Standards
Personal Responsibility for Actions
Review Threats - Expert
Review Detection / Mitigation - Expert
Responses
Range Simulation / Interaction / Review (3 Scenarios)

Cyber Skill Level: High

Duration: 2 full days

Frequency: 2x per year

Cost: On Site (Group of 5) $13,000.00 + Expenses

Responsibilities: Tier 2 and 3 analysts tackle the difficult situations that tier 1 analysts escalate to them. This includes complicated malware scenarios such as file-less and multi-pronged malware attacks. These expert analysts are in charge of complex procedures such as deep incident analysis, root cause analysis, determining if and which assets have been affected, forensics and reverse engineering.

Challenges: Tier 2 and 3 analysts need to keep their skills sharp and up-to-date so that they can deal with the complicated, ever-shifting threats that come their way. Therefore, these experienced analysts must focus on constantly improving the broad skillset needed to do their job, which includes using the latest advanced tools and systems. Additionally, it can be challenging to work with Tier 1 analysts in a smooth and reliant way that ensures that the right group is tackling each issue.

Training: Tier 2 and 3 analysts are responsible to investigate and close the more serious cyber incidents. These are our professional cyber heros, always under pressure to save the day when faced with new threats. They must ensure that their actions are choreographed with perfect precision, which is nearly impossible without a system of ongoing training. Training focuses on simulating full-scale attacks that are customized to the specific organization so they experience the scenarios that pose the biggest threat to their network. Analysts learn to handle multiple systems and alerts during crisis, improve teamwork and knowledge in procedures, all of which will help them make it through incidents with as little collateral damage as possible.

Skill Workshops: This is a series of hands on workshops, presenting real environments with dedicated scenarios to improve particular skills that are critical to withstanding attacks, for example mobile forensics and ransomware reversing.

6. IT Department

WHO: IT Department

WHAT: Coordinate Cyber Response Drills

Background:
Current Corporate Policies / Standards
Enforcing Policies and Standards
Personal Responsibility for Actions
Review Threats / Entry level - Journeymen
Review Detection / Mitigation - Journeymen

Cyber Skill Level: Medium

Duration: 4 hours

Frequency: Once per year

Cost: On Site (Group of 10) $5,000.00 + Expenses

Skill Level: Medium

Responsibilities: The IT department works with the SOC team, ensuring that response processes are in place, enforcing security protocols in the network and supporting cyber technology in the organization.

Challenges: Coordinating their work with the SOC in order to allow operations to run smoothly may run counter to what the IT department wants to focus on.

Training: Training sessions help IT staffers understand their role in upholding and enforcing security policies. Sessions focus on creating smooth handovers, escalation protocols, crisis management and communication channels.

7. General Employees

WHO: General Employees

WHAT: Cyber Security Awareness & Prevention

Background:
Current Corporate Policies / Standards
Personal Responsibility for Actions
Review Threats / Entry level
Secure User Interaction

Cyber Skill Level: Low

Duration: 2 hours

Frequency: 2x per year

Cost: On Site (Large Group) $15,000.00 + Expenses

Skill Level: Low

Responsibilities: This group must be aware of the threats that exist.They must know that phishing emails, malicious links, fraudulent websites and rogue employees are all very real, and if they aren't careful, they might end up exposing their entire organization to a wide scale attack.

Challenges: Security is often the very last thing on this group's radar. They are not oriented towards security threats and their performance isn't measured by keeping their organization secured. Bottom line - security is not their focus and they are at high risk for becoming victims of human engineering tactics.

Training: Your general employees need to become educated in the very basics of cyber security awareness; they must learn what phishing emails look like, how to recognize fraudulent websites, how to create solid passwords and how to spot potentially malicious insiders. Sessions focus on learning the threat landscape and impact and learning to detect, avoid and report suspicious activity.

8. External Contractors

WHO: : External Contractors

WHAT: Cyber Security Awareness & Prevention

Background:
Current Corporate Policies / Standards
Personal Responsibility for Actions
Review Threats / Entry level - Entry
Secure User Interaction

Cyber Skill Level: Low

Duration: 2 hours

Frequency: 1x per year

Cost: Same as "General Employee" training. Consider inviting contractors to join planned trainings.

On Site (Large Group) $15,000.00 + Expenses

Skill Level: Low

Responsibilities: The responsibility of any external contractor you might engage with is to keep supply chain protocols and security procedures. Unfortunately, external contractors can easily become points of entry for cyber attacks.

Challenges: The most major challenge here is that it's very hard to control what your third party vendors do because they aren't bound by, or even fully aware of, your organizational rules and protocols.

Training: Partner security training should focus on reviewing security protocols and common "dos and don'ts".

Cybersecurity Training Resources and Tools

The Cyberbit Range Training and Simulation platform allows you to create customized training scenarios to meet the specific needs of each group across your organization. You can provide your employees with hyper realistic training scenarios that will dramatically reduce security errors and improve their performance in the face of crisis and daily tasks.

More Options for Medium to Advanced Users

Open Cyber Challenge: Developed by the University of Rhode Island, this free, configurable platform gives users the opportunity to test their skills in different simulated scenarios.

Cybrary: An open source e-learning program with over 30 on-demand courses that include lectures, study guides and interactive demonstrations.

InfoSec Institute: With close to 20 years of experience in cyber security training, the InfoSec Institute provides a wide range of top notch online courses.

Sans: One of the largest sources for online security training, also offers a Master's Degree in cyber security.

Options for Non-Technical Staff

CyberSecurity MOOCs: These huge online courses cover every topic imaginable in cyber security making them a great resource for beginners and advanced users as well.

Future Learn's Introduction to Cyber Security Course: An 8 week interactive course designed especially for your non-tech staff to further enhance their awareness.

Phishing Simulators:

Infosec Institute has a helpful list of 9 free phishing simulation tests.

Overcoming the Cyber Skills Crisis

In today's ever-changing cyber threat landscape, giving your organization the best shot at remaining secured depends on each and every person responding to every breach and attempted breach in the most optimal manner. This can't and won't happen without putting in the time and effort it takes to ensure that every employee, across the organization, is well practiced in relevant security skills.

You may never be able to hire all the security professionals you dream of but with the right resources and training, you'll find you never really needed them in the first place. To find out more about giving all your employees the skills they need to keep your organization secured, contact our Cyber Range sales team today.

ABOUT CYBERBIT™

Cyberbit provides a consolidated detection and response platform that protects an organization's entire attack surface across IT, OT and IoT networks. Cyberbit products have been forged in the toughest environments on the globe and include: behavioral threat detection, incident response automation and orchestration, ICS/SCADA security, and the world's leading cyber range. Since founded in mid-2015 Cyberbit's products were rapidly adopted by enterprises, governments, academic institutions and MSSPs around the world. Cyberbit is a subsidiary of Elbit Systems (NASDAQ: ESLT) and has offices in Israel, the US, Europe, and Asia.

www.cyberbit.com | sales@cyberbit.com

CYBERBIT
PROTECTING A NEW DIMENSION