Cybersecurity Incident Response Exercise Guidance

Information security and privacy incidents are becoming more frequent. According to the CyberEdge Group *2021 Cyberthreat Defense Report*, 2021 "…saw the largest increase in successful attacks within the last six years."[1] In addition, it stated that "Over time, cybersecurity professionals have come to realize that it's more of a question of when their organization will be victimized by a data breach than if." As a result, it is more important than ever to train incident response teams (IRTs) to recognize, handle and respond to cybersecurity (and privacy) incidents.

Organizations must review cybersecurity threats and attack vectors, understand the importance of the incident response plan (IRP), review response activities, conduct tabletop exercises, analyze the exercises to determine areas for improvement, manage reporting and conduct IRP maintenance.

IRP

The IRP provides a road map for implementing the incident response capability as defined by the organization's mission, size, structure, functions, strategies and goals. In addition, it identifies the organizational approach to incident response, contains communication information and defines the metrics associated with the incident response capability. The topics of information security and privacy are usually intertwined but can be addressed separately—each with their own plan.

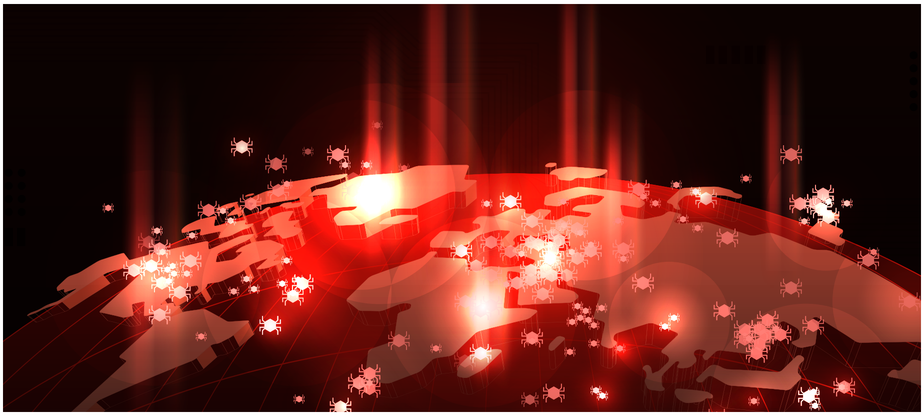
Because of the varied types of organizations (e.g., large, medium, small, international), the IRT communication requirements will vary. Participants in incident communication can include Internet service providers (ISPs); software and support vendors; incident reporters; law enforcement; customers, constituents and partners; media; and other IRTs. IRTs can be centralized, with one team at a central headquarters; distributed, with multiple teams to support different time zones or locations; coordinated with a headquarters that manages multiple teams; partially outsourced; fully outsourced; or using internal staff. All of these considerations must be included in the IRP.

Cybersecurity Attack Vectors

The group responsible for the plan will vary depending on the organization, but the threats and attack vectors will not. **Figure 1** is an analysis of the cyberattack vectors that can aid in developing descriptive exercise scenarios.[2, 3] It contains examples and descriptions, vector objectives, and who or what identified an active attack. Corrective actions to address the problems are not included.

Tabletop Exercises

A major concern with implementing an IRP is whether the plan will work. To ensure that it does, tabletop exercises should be conducted at least annually. Tabletop exercises are defined as:



Larry G. Wlosinski, CISA, CRISC, CISM, CDPSE, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP
Is a senior consultant at Coalfire-Federal. He has more than 22 years of experience in IT security and privacy and has spoken at US government and professional conferences on these topics. He has written numerous magazines, newspaper and journal articles; reviewed various ISACA® publications; and written questions for the Certified Information Security Manager® (CISM®) and Certified in Risk and Information Systems Control® (CRISC®) examinations.

Figure 1—Cybersecurity Attack Vectors

Cyberattack Vector	Examples/Description	Objective	Problem Identifier
Malware	Virus, worm, trojan horse, spyware, rootkit software	Data theft, password stealer, network or system compromise	Antivirus software; intrusion detection system (IDS)
Phishing (includes spear phishing)	Deceptive malicious email that targets organizational users and uses attachments or malicious links to plant malware	Network or system access; data breach	User
Ransomware (includes doxing)[a]	Extortion (data are deleted or encrypted unless ransom is paid)	Blackmail for ransom	Ransomware announcement
Denial of service (DoS) (includes distributed DoS [DDoS])	Overwhelm network device or server to prevent access or usage	Network or system disruption	Network administrators via network monitoring system
Compromised, weak or stolen credentials	User login account and password	Data breach	Forensic investigation
Malicious insiders	Disgruntled employee who exposes private information	Revenge, embarrassment	Management, United States Computer Emergency Readiness Team (US-CERT)
Third- and fourth-party vendors	Suppliers, cybersecurity partners	Obtain competitive information	Network monitoring system; log management system
Missing or poor encryption	Data at rest, data in motion	Gain access to data	System assessment
Device misconfiguration	Servers, network devices, mobile computing devices	Obtain access to device and data	System assessment
Unpatched vulnerabilities	Servers, network devices, mobile computing devices	Obtain access to device and data	Patch management system
Structured Query Language (SQL) injections	Manipulate database servers to expose information	Gain access to data	Penetration tester
Cross-site scripting	Inject malicious code into a comment	Gain access to system, network and data	Penetration tester
Session hijacking	Intercepted session cookies	Gain access to data	User
Man-in-the-middle (MitM) attacks	Public Wi-Fi networks	Gain access to network	Intrusion prevention system (IPS)
Brute-force attack	Trial-and-error attempts to gain access to network or system	Gain access to system, network and data	Log management system

Source: (a) Wlosinski, L. G.; "Ransomware Safeguards and Countermeasures," *ISACA® Journal*, vol. 4, 2020, *https://www.isaca.org/archives*

Discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.[4]

Exercise Purpose

The purpose of tabletop exercises is to understand the roles and responsibilities of the support team, response priorities, order of events, roles of the various plans, communication requirements, and the role and use of the tools at the team's disposal. Participants also learn how to react to various scenarios, verify procedures and determine what is missing from plans.

The agenda of the tabletop exercise should include an introduction of participants, a review of the exercise scope and logistics, scenario walk-through, a review of testing questions, the exercise, and survey completion. Afterward, the facilitator and data collector discuss the observations, survey responses and write an after-action report (AAR).

The AAR should include the date and time of the exercise, a list of participants, scenario descriptions, findings (generic and specific), observations with recommendations, lessons learned and an evaluation of the exercise (strengths, weaknesses, lessons learned). An executive briefing (i.e., exercise recap and team evaluation) may also be required if requested.

> "PARTICIPANTS ALSO LEARN HOW TO REACT TO VARIOUS SCENARIOS, VERIFY PROCEDURES AND DETERMINE WHAT IS MISSING FROM PLANS."

Exercise Preparation

Once the IRP has been written, the manager responsible for the IRP can prepare for the exercise. Assuming that the exercise participants have had some kind of training, preparation activities should include:

- **Design the exercise**—Scenarios specific to the systems (e.g., enterprise, security operations center [SOC], region) and support activities (e.g., network monitoring, log file analysis, intrusion detection, digital forensics) are created. The purpose of the SOC is to lock traffic and requests, monitor systems, keep ingress from the Internet domain, protect internal corporate systems, respond to investigations, perform digital forensics, analyze data and reports, and satisfy reporting requirements. The SOC uses tools such as Splunk, elastic search, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), a security information and event management (SIEM) system, and cyberthreat intelligence (CTI), if available.
- **Determine the topics**—The exercise topics can be selected by attack vector, type of data (e.g., network, privacy, organization sensitive, system specific) and direction of attack (i.e., external or internal).
- **Determine the scope**—The scope of the exercise (i.e., roles and responsibilities) can range from just the response team to the system administrator, security staff, organizational partners and vendor. The exercise can be at the management or operational level.
- **Identify the objectives**—Objectives should be oriented to the purpose and content of the plan that will be exercised. Having pertinent objectives aids in exercise participation.
- **Identify the participants and staff**—This activity is intended to validate the operational procedures of the plan and the tasks of the associated personnel (who should all be invited). An exercise facilitator and data collector are assumed to be part of the exercise.
- **Coordinate logistics**—Logistical concerns include the date and time, location (e.g., conference room, remote/virtual session), supporting equipment (e.g., laptops), placards, refreshments, meeting invitations, and supporting/reference documents (e.g., IRP).
- **Develop the material**—The material can include presentation slides, a participant guide, facilitator guides and survey questionnaire. The questionnaire should ask about issues not discussed, plan and exercise strengths and weaknesses, information gained from the exercise, and suggested improvements to the exercise.

Exercise Scenarios

The development of information security and privacy incident scenarios for exercises should

Enjoying this article?

- Read *Security Incident Management Audit Program. www.isaca.org/security-incident-management-audit-program*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

include considerations for scope and objectives, but it should also focus on the intent of the plan. **Figure 2** shows examples broken down by area of focus, with the identifier of the incident and type of data.

Scenario discussion questions can cover plan activation, ownership and location. Personnel involvement (i.e., who would be contacted and how) and management action should be discussed. A review of the procedures (i.e., forensics, backup, data storage, retrieval, restoration) should also be included, along with "what if" questions.

Conducting the Exercise

There are six main activities in the incident response life cycle: preparation, identification, detection and analysis, containment, eradication and recovery, and post-incident activities. They all should be discussed in one or more tabletop exercises as questions presented by a facilitator. The activities should include:

1. **Preparation**—The topics discussed in the preparation portion of the exercise include policies and procedures, critical documents, points of contact (i.e., IRT, external partners, internal partners), tools, resources, document and information accessibility, and continuous monitoring.
2. **Identification**—Points to discuss during the identification phase are criteria for declaring the impact level of the incident, data to be collected, incident severity and third-party data (if applicable). Once this has been determined, discussion of the data and the level of risk to the organization (internal and external ramifications) is necessary.

Figure 2—Sample Incident Response Exercise Scenarios

Area of Focus	Scenario	Incident Identifier	Data Type
Unauthorized access	Someone has assumed the identity of an administrator and has accessed the network remotely (could be password cracking or key logging)	SIEM system	Any
Access, data breach	Multiple simultaneous/ongoing attacks	Network activity	Any
Compromise	Telecommuting compromise via social engineering	SIEM	Sensitive information
Computing device	Organization-issued mobile/wireless device contains malware	Vulnerability scan	Any
Data breach	Compromised database server	IDS	Sensitive information
Data breach	The backup media storage vendor has been compromised and some backup files were taken	Storage vendor	Any
Data breach	Ransomware has affected the system data files and backups	Malware	Any
Data breach	Combined cloud system provider (CSP) and SOC exercise	Any	Any
Network compromise	A device (e.g., router, switch domain name system [DNS]) has been found to be compromised	IDS, SIEM	Network
Network compromise	Someone (insider or visitor) has installed a wireless access point (WAP) into the network	System assessment	Any
Service	Worm and DDoS agent infestation	Antivirus software	Privacy
Unauthorized sharing	Sharing paper or electronic documents containing privacy information with individuals who are not authorized to access them	Supervisor	Privacy

3. **Detection and analysis**—The detection and analysis discussion should cover investigation strategy and priorities, team assignments (i.e., roles and responsibilities), scope of the incident (e.g., network, internal servers, partners, customers), tool report findings, information sharing among the team and others, management reporting, government reporting, and sources of information (e.g., malware descriptions and remediation advice, vendor resources).
4. **Containment**—The containment portion of the exercise includes discussion on how containment is to be achieved, the gathering of forensic information and the removal of data that may have been published on the Internet.
5. **Eradication and recovery**—The eradication and recovery discussion should focus on vulnerabilities to the processing environment (e.g., points of access or entry), cleaning and restoring infected devices, access and connectivity concerns, patching, device and software reconfiguring, and any additional weaknesses uncovered.
6. **Post-incident**—The post-incident discussion should be about changes to continuous monitoring, lessons learned and improving governance. The lessons learned apply not only to the organization but also to partners and cloud providers. An exercise survey could be used to obtain additional concerns, comments and recommendations.

IRP Maintenance

Maintaining the IRP requires periodic reviews at least annually, particularly for the areas that may change frequently. The areas that may change include point of contact information, links to supporting documents, and procedures and policy. Information gained from the exercises can be used to update the plan.

Conclusion

It is important for those who write, maintain and oversee the IRP to understand its purpose, how to test/exercise the support teams, the preparation components and activities, sample scenarios, reporting, and plan maintenance. It is up to each organization to use this information to improve the level of security and privacy of the data in their organization, and thereby ensure a quick and effective response to the many types of cybersecurity incidents that can harm or cripple them.

Endnotes

[1] CyberEdge Group, *2021 Cyberthreat Defense Report*, USA, 2021, *https://resources.perimeterx.com/c/2021-cyberthreat-defense-report?x=OxBXZ2*

[2] Balbix, "Eight Common Cyber Attack Vectors and How to Avoid Them," USA, *https://www.balbix.com/insights/attack-vectors-and-breach-methods/*

[3] Tunggal, A. T.; "What Is an Attack Vector? 16 Common Attack Vectors in 2021," UpGuard, 25 May 2021, *https://www.upguard.com/blog/attack-vector*

[4] Grance, T.; T. Nolan; K. Burke; R. Dudley; G. White; T. Good; Special Publication (SP) 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, National Institute of Standards and Technology (NIST), USA, 2006, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf*