Ashpool

Cyber Operations

Incident Response Checklist

Incident Origin Information							
Incident #:		Date Reported:			Date of Event:		
Theft?	Yes No	Time Reported:		Time Zone	Time of Event:		Time Zone
If Theft, Police Report ID:							
Reporting Party:	Name:		Department:		Title:		
	Cell Phone:		Email Address:				
Responding Party:	Name:		Department:		Title:		
	Cell Phone:		Email Address:				
Location:		Object:		Responsible Department:			
Inventory #:		Department Contact #:		Department Manager:			
Summary of incident:							

Compromised System Information					
Computer Name(s):		IP(s):		OS:	
Software Present:				Contain PII:	Yes No
Accessible Network Shares:			Computer Used Primarily By:		
Incident Type:	Malware DDoS Web-Application-Attack Phishing Policy-Violation Other				
If Web App Attack:	XSS Broken-Access-Control SQL-Injection Unpatched Other				
If Other, describe:					
Accounts Logged On to Computer:					

Web Attack Information

Originating IP(s):		Affected IP(s):	
Originating Domain(s):		Affected Domain(s):	
Breach Detected:	Yes No	Attack Type:	
Information Regarding Attack:			

Malware Information

Name of Malware:		Malware Family:	
AlienVault Link:		VirusTotal Link:	
Any.Run Link:		TrendMicro Link:	
MD5 Hash of File(s)			
IP(s) Associated w/ the Malware:		URL(s) Associated w/ the Malware:	
How was it Detected:			
Impact Characteristics:		Summary of Malware:	
Actions Taken:			
# Of Compromised Systems:			

	Timeline of Incident Response Activities	
Date:	Time:	Event / Description:

Analysis			
Directly Impacted Systems:		Downtime of Direct Systems:	
Indirectly Impacted Systems:		Downtime of Indirect Systems:	
IT’s Response to the Incident:		Future Impact on IT Services:	
Next Steps:			
Changes Made:			
Incident State:	Active Open Closed		

Chain of Custody		
From:	To:	Date:

Communications Record

Communication Type:	To:	From:	Date:	Time:	Description:

Lessons Learned

Summary of Lessons Learned:				
Incident or Risk	Lessons Learned	Actionable Items	Owner of Item	Status

Revision Table

Date Revised	Author	Revision Description
1/17/2022	Evan Read	Created the document
1/26/2022	Evan Read	Updated per Prof. Egeberg’s recommendations

Sources:

[1] J. Creasey and I. Glover, “Cyber Security Incident Response Guide,” CREST, 2013. Accessed: Jan. 26, 2022. [Online]. Available: https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf.

[2] U.S. Department of Health and Human Services, “Incident Handling Checklist.” Accessed: Jan. 26, 2022. [Online]. Available: https://www.hhs.gov/sites/default/files/incident-handling-checklist.pdf.

[3] Center for Internet Security, “Cyber Incident Checklist,” *CIS*, 2022. https://www.cisecurity.org/white-papers/cyber-incident-checklist/ (accessed Jan. 26, 2022).

[4] Spencer Fane LLP, “Cyber Incident Response Checklist,” Spencer Fane LLP. Accessed: Jan. 26, 2022. [Online]. Available: https://www.spencerfane.com/wp-content/uploads/2019/01/Cyber-Incident-Response-Checklist.pdf.

[5] Infocyte, “Incident Response Planning: A Checklist for Building Your Cyber Security Incident Response Plan,” *Infocyte*, Nov. 07, 2019. https://www.infocyte.com/blog/2019/11/07/incident-response-planning-a-checklist-for-building-your-cyber-security-incident-response-plan/ (accessed Jan. 26, 2022).

[6] J. Carson, “Cyber Incident Response Checklist and Plan: Are You Breach-Ready?,” *Thycotic*, May 27, 2021. https://thycotic.com/company/blog/2021/05/27/cyber-incident-response-checklist/ (accessed Jan. 26, 2022).

[7] Texas Department of Information Resources, “TEXAS DEPARTMENT OF INFORMATION RESOURCES Incident Response Team Redbook,” 2020. Accessed: Jan. 26, 2022. [Online]. Available: https://dir.texas.gov/sites/default/files/Incident%20Response%20Template%202018.pdf.

[8] M. Blair, “Computer Security Incident Response Plan,” Feb. 2015. [Online]. Available: https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf.

[9] RIC One, “Cybersecurity Incident Response Plan CREATED,” 2019. Accessed: Jan. 26, 2022. [Online]. Available: https://www.esboces.org/cms/lib/NY01914091/Centricity/Domain/440/Incident%20Response%20Plan%20Template.6.5.19.pdf.

[10] Orion Cassetto Director, Product Marketing, “Incident Response Plan 101: How to Build One, Templates and Examples,” *Exabeam*, Nov. 21, 2018. https://www.exabeam.com/incident-response/incident-response-plan/ (accessed Jan. 26, 2022).

[11] CrowdStrike, “Incident Response [Beginner’s Guide] | CrowdStrike,” *crowdstrike.com*, May 06, 2021. https://www.crowdstrike.com/cybersecurity-101/incident-response/ (accessed Jan. 26, 2022).