

Assignment 2.1: Compromised Network Indicators and Risk Mitigations

Joshua A. Wortz

University of San Diego

CSOL-560

Dr Varma

11/03/2025

Threat	Vulnerability	Asset & Consequences	Risk	Solution
Home router compromise (unauthorized access / password change)	Weak or default admin credentials, outdated firmware, and remote management enabled.	Router and all connected devices. Loss of confidentiality and integrity of network traffic; an attacker can alter DNS or lock out a user.	High	Change default credentials; disable remote admin; update firmware; enable WPA3; review device list; reset router if suspicious activity is seen (CISA, 2021; NIST, 2020).
Malware infection on endpoints	Unpatched OS or applications; weak endpoint protection; user executes malicious links.	Laptops, phones, IoT devices. Data theft, keylogging, webcam activation, or persistence mechanisms.	High	Maintain endpoint protection and automatic updates; limit admin rights; disconnect infected systems; reimage from trusted media (NIST, 2020; Paganini & Martins, 2017).
Browser / DNS redirection attacks	Compromised router or browser settings; malicious extensions.	Online accounts and financial data. Redirected to credential-harvesting sites.	High	Verify DNS configuration; reset router; use DNS-over-HTTPS; remove untrusted extensions; apply browser updates (CISA, 2021; NIST, 2020).
Ransomware infection	Opening malicious attachments, outdated software, and a lack of backup discipline.	Local and cloud-synced files. Data encryption and extortion risk.	High	Maintain offline and cloud backups; isolate infected hosts; rebuild from clean image; use email filtering and user awareness training (NIST, 2018; Paganini & Martins, 2017).
Online account compromise	Reused or weak passwords, lack of MFA, and phishing	Cloud email, banking, and work accounts. Credential theft and identity fraud.	High	Enforce MFA; use password manager with unique credentials; review login activity; reset

Threat	Vulnerability	Asset & Consequences	Risk	Solution
	exposure.			credentials after incidents (CISA, 2021; NIST, 2020).
IoT device compromise / pivot attack	Default credentials, poor vendor security, and no segmentation.	Smart home devices and the network as a whole. Used for lateral movement or botnets.	Moderate–High	Segment IoT network (VLAN/guest SSID); disable remote access; update firmware; remove unused devices (Huang et al., 2019; NIST, 2020).
Unauthorized Wi-Fi access or rogue AP	Weak encryption or shared passwords; WPS enabled.	Personal data and network integrity. Man-in-the-middle interception or data theft.	Moderate–High	Use WPA3, disable WPS, change SSID/password periodically, and monitor MAC addresses (CISA, 2021; NIST, 2020).
Phishing and social engineering attacks	Users are deceived into disclosing credentials or installing malware.	Personal identity data; network credentials.	High	Continuous user awareness training; deploy email filtering; verify sender authenticity before link clicks (NIST, 2018; Paganini & Martins, 2017).
Incomplete remediation after compromise	Only partial cleaning or password changes; no full system reset.	Entire network; lingering attacker persistence.	High	Perform complete device resets, reimage OS, update all credentials, and validate logs post-incident (NIST, 2020; CISA, 2021).
Loss of forensic evidence during response	Immediate reboot or factory reset before triage; no centralized logs.	Volatile memory and event logs. Limits the ability to trace intrusion.	Moderate	Centralize logs; pause device before erasure; seek expert guidance; document timeline of events (NIST, 2018; CISA, 2021).

References (APA 7th Edition)

Cybersecurity & Infrastructure Security Agency. (2021). *Best practices for securing your home network* [CSIA Guide 21-01]. U.S.

Department of Homeland Security.

https://www.cisa.gov/sites/default/files/publications/CISA_Home_Network_Security_Tips.pdf

Huang, W., Zhao, Z., Zhang, W., & Cao, J. (2019). A survey on IoT security: Application perspectives. *IEEE Internet of Things Journal*, 6(5), 8205–8218. <https://doi.org/10.1109/JIOT.2019.2928889>

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).

U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.04162018>

National Institute of Standards and Technology. (2020). *Guide to enterprise telework, remote access, and bring your own device*

(BYOD) security (SP 800-46 Rev. 2). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-46r2>

Paganini, P., & Martins, A. (2017). Home network security risks and mitigation strategies: A systematic review. *Computers &*

Security, 70, 331–347. <https://doi.org/10.1016/j.cose.2017.06.009>