



Riskigy vCISO Team Resources: Cybersecurity Tabletop Exercise Series

Our Scenarios to Help Prepare Your Incident Response Team

Exercise Title:

Unauthorized Access

TTE Scenario:

It has come to your attention that the social media website of your organization has been infiltrated. An international terrorist group identifying themselves as the "Uproar Cyber Force" has expressed their displeasure towards American politics through public news sources. They have proclaimed to have conducted cyber attacks on several government organizations. It has been discovered that the official social media accounts of your organization have been breached, and an individual is utilizing them to broadcast notifications to the public alleging that the organization has been compromised by the Uproar Cyber Force.

Cyber Attack:

The cyber attack in this situation is a social engineering attack, specifically a phishing attack. The attacker has successfully tricked an employee of the organization into providing their login credentials, which allowed them to gain unauthorized access to the official social media accounts of the organization. The attacker then utilized these accounts to spread false information and cause chaos. This is a common tactic used by cybercriminals to gain access to sensitive information or cause reputational damage to an organization.

Incident Impact:

- Financial losses: Unauthorized access attacks can result in significant financial losses, such as the cost of remediation, lost productivity, legal fees, and the impact of reputational damage on revenue.
- Legal and Compliance Issues: Unauthorized access can result in legal and compliance issues, especially if the organization is subject to regulatory requirements such as GDPR, HIPAA, or PCI-DSS.
- Data loss: Attackers may modify or delete critical data.
- Malware Infection: Once an attacker gains unauthorized access, they may install malware on the system to control it remotely or to gain further access to other systems in the network.



CYBERSECURITY & TECH LEADERSHIP FOR START-UP, EMERGING & BEYOND

vCISO vCTO vCIO Consultants Experts

Lesson to Learn:

- How would you be alerted if account takeover notifications were being sent from your social media account?
- What policies or practices do you have in place to address the situation?
- What steps will your organization take?
- Did an employee put the organization at risk?
- What can be done so that this can be prevented?