SUPPLY CHAIN COMPROMISE: BLIND ADMINISTRATION

You can't always anticipate a data breach. What do you do when the unexpected happens at a high-security organization? What if national secrets are now in the hands of your adversaries?

You work in a leadership role at Cybersecurity Command. Cyberattackers have stolen red team tools from IceNose, a company that provides your software. The vector of attack is disclosed as an update to the specific LuneTyphoon program which your company uses. After a technical investigation, it's revealed that you too have been affected. Foreign adversaries could now have access to your cyber weapons and secrets, pertinent to national defense. How will you navigate the political and reputational fallout from this crisis?

SECTORS	VECTORS	ACTORS	MOTIVATIONS	IMPACTS	NON-TECHNICAL SKILLS
Financial Services	Insider Threat	Organized Criminals/ Cyber	Financial	Employees	Situational Awareness
Healthcare	Ransomware	Criminal Groups	Political	Customers	Effective Leadership
Transport, Logistics & Supply Chain	DOS	Political/Social Activists	Publicity for a Cause	Operations	Rational & Intuitive Decision Making
Energy & Infrastructure	Cloud	Disgruntled Employees/Former	Personal Malice	Shareholders	Communications
Government	Vulnerability Disclosure/ Reporting	Employees/ Customers	Commercial Advantage	Financial/ Commercial	Stress Management
	Social Engineering, Fear Exploitation, Covid	Terrorist Groups	Cause Operational Delays or Disruption	Reputational	Teamwork
	Data Breach	State Actors		Legal	
	Remote Working			Regulatory	
	Electoral Fraud				

IMMERSIVELABS

CRISIS SIM SCENARIO

This scenario is based on the SUNBURST attack and how it affected governmental agencies. It focuses on the potential political, diplomatic, reputational and security impacts to a government agency, forcing the player to navigate the loss of national secrets of strategic security importance.

Non-technical skills tested in this simulation include communication, effective leadership and stress management.

The scenario begins when IceNose, a cybersecurity firm, reveals it has been attacked by a sophisticated group, possibly led by a nation state. The network management technology provider LuneTyphoon provided the entry point for the attack and Cybersecurity Command has been affected.

The scenario then moves into media and partner management. The incident at the center of this scenario is that one of your cyber weapons has potentially been compromised, along with other national secrets.

WHO IS IT AIMED AT?

This scenario is aimed at an executive-level crisis management team, particularly those who work in the public sector. It will also benefit executives in any organization who are required to support their corporation's response to a major cyber breach where critical data may have been compromised.

WHY HAVE WE COVERED THIS?

The SolarWinds SUNBURST attack is one of the biggest cybersecurity crises in recent years and has affected a number of government bodies across the US and UK. As the compromise came from a trusted supplier, there was nothing that the affected organizations could have done to anticipate or prevent it. Therefore, recovery and post-incident decisions are at the crux of this scenario. Stress testing teams allows them to practice their response to an incident such as this, and will help build muscle memory, resulting in a more efficient performance in the instance of a real crisis.