IMMERSIVELABS

CRISIS SIM SCENARIO

RANSOMWARE: LEFT OUT IN THE COLD

Should you ever pay the ransom? What if it were a matter of life and death?

In the peak of a brutal winter and a global pandemic, power distribution company Energon gets hit by not one, but two Netwalker ransomware attacks, causing power-outs across the country. It's up to you to prioritize tasks, appoint leaders, push out comms, and of course decide whether to pay the malicious hackers. Most importantly, will you be able to prevent fatalities?

WHAT IS THIS SCENARIO ABOUT?

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				

This scenario focuses on a ransomware attack in the energy sector. Its overall impact hits almost every category, causing havoc on operations, customers, the company's reputation, and much more. Although not outwardly specified, this attack was carried out by an organized cybercriminal group, whose main motivations are financial gain and the disruption of operations.

WHAT SKILLS DOES THIS SCENARIO TEST?

This scenario is aimed at an executive-level crisis management team. Most of the main non-technical skills are tested in this scenario, with a mix of challenges and decisions designed to examine situational awareness, effective leadership, rational and intuitive decision making, and communications.

WHY IS THIS SCENARIO IMPORTANT?

The energy sector is being attacked with ransomware more frequently. During these attacks, we've come to see an over-reliance on insurance policies, with companies paying out to malicious groups far too quickly.

The worst case scenario when looking at a crisis in, say, a financial services organization is a data or privacy breach. However, when one crosses the line into the energy and infrastructure sectors, the decisions may literally come down to life or death.

WHY SHOULD BUSINESSES CARE?

According to McKinsey's 2020 Building Resilient Operations report, ineffective or delayed responses to major crises, including cyber crises, can lead to reductions of as much as 15% of gross earnings. By practicing and stress-testing your teams, business responses will be quicker, reducing the overall impact of the attack and allowing them to get back to 'normal' faster.

The presence and reputation of companies is more prevalent now than ever, thanks to social media. Five or ten years ago, a singular fatality caused by a company's negligence may not have been disclosed or even heard about. Nowadays it spreads like wildfire. Companies need to be more socially conscious of their customers, responsibilities, and employees.