RANSOMWARE: DOUBLE BARREL

THREAT RESPONSE CRISIS SIMULATION

You are part of the executive crisis management team at Patriot Pipelines Inc., one of the largest fuel distribution companies in the US, which predominantly serves the East Coast.

Patriot transports and distributes crude oil for domestic and commercial use. It is also a critical supplier of fuel to the US military and emergency services. Patriot's Alpha 24 pipeline carries 2.75 million barrels a day – 45% of the East Coast's supply of diesel, petrol and jet fuel.

In May 2021, Patriot's network was hit by a severe ransomware attack by the APT threat group DarkSide, which operates using a model dubbed "ransomware as a service" (RaaS). The attack was part of a double-extortion scheme – one of the group's known methods. It threatened to leak Patriot's stolen data on the internet while encrypting and locking information on Patriot computers inside the network until a ransom was paid.

In this crisis simulation, you will navigate the challenges that arise when a cyberattack has multiple potentially severe operational consequences.

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				
	Impersonation				
	Physical Security Breach				

THE ATTACK

Patriot has two connected core networks operating on an "air gap" principle that allows them to work independently: one for IT and corporate systems and one for operational process controls. The latter uses automated systems to control and monitor the flow of fuel from refineries and tank farms into the pipes, and subsequently from the pipes into tanks and transportation facilities of suppliers and distributors at the other end. Patriot uses only Cisco ASA Firewalls to protect its data, which have been vulnerable in the past.

You're working hard to fix the problem, but the oil supply to nearly 150 million customers is at risk. The government has approved emergency domestic fuel transportation measures and has immediately increased its oil import quota, destabilizing international oil prices in the process.

Although on separate networks and not knowingly affected, Colonial Pipeline, on whom this sim is based, decided to shut down the operational network to prevent the attackers from getting further into its systems – despite the air gap between the networks – halting the supply of fuel to 10 southeastern states in the process. Will you do the same?

SO WHAT?

This scenario was built in response to the May 2021 DarkSide cyberattack on Colonial Pipeline. It is designed to test any infrastructure company or energy provider's response to a major cyber breach, with the potential for direct and indirect operational consequences. The scenario is designed for leadership members and deputies of both cyber incident management and executive crisis management teams. It challenges participants' decision making, situational awareness and communications skills, as well as their adherence to, and knowledge of, best practice incident response strategies and tactics.

This particular incident also highlights the risk ransomware can pose to national industrial infrastructure, and how collaboration between business and government in this area is critical.

In addition, participants are faced with a number of technical wicked problems: whether to shut down a network, how to prioritize fuel transportation according to existing and new legislations, risk assessments, and how to deal with media requests for information when you still know very little; all of this while balancing the crisis response performance indicators of time to return to operations, corporate reputation, regulatory scrutiny, and financial loss.

The situation appears to be under control – but for how long?

Users can prepare for this scenario by learning more about the attackers in the Immersive Labs platform:

Darkside Overview Lab