GettyImages/PeopleImages: 5140497

What to do when hacker attack your port's business?

A cautionary tale

Dustin Eno, COO and crisis response manager for Navigate Response; and ***Devin Sirmenis***, managing director of Corporate Resilience for Witt O'Brien's, talk through a fictional cyber attack and steps ports need to take in a similar situation to ensure business continuity

Before leaving on a holiday with his family, fictional Port of Nirvana executive director Scarn diligently completed some outstanding correspondence, tasked others internally on a few critical items, and finished looking at some links from colleagues. Scarn turned on his out-of-office notification, closed his laptop and locked it in his office, and left for his holiday with peace of mind.

Captain Dimitrius was on board the vessel *Triumphant* at Nirvana port, offloading cargo. He was writing a reply to an article he had just read from Scarn, calling attention to the failure of most ports and shipping companies to complete implementation of business continuity, crisis management, and cyber security initiatives now being heavily enforced under the International Ship and Port Facility Security Code.

Dimitrius outlined his thoughts on how he would prioritise investments across purchases, maintenance, plans, training, security drills, and equipment such as x-ray scanning, biometrics, and computer security software. Proud of his writing, he expanded the distribution list and included a dozen other ports and global shipping companies.

Things were busy on board *Triumphant*. Vessel and port crew swapped data with each other, inserting and removing flash drives in ageing laptops as *Triumphant* departed after completing cargo operations.

Port of Nirvana was slammed; running at full capacity. Crane operator Johansen had been at it for hours; methodically lowering containers into hulls, stacking them

Navigate Response: 5140495

> Public and stakeholder perceptions form quickly. Protect your reputation immediately
>
> **Dustin Eno**
>
> *COO and crisis response manager for Navigate Response*

deliberately and with the ease that comes with years of on the job. After grabbing a new container, Johansen started to move it into position, but the joystick stopped responding the way it should have. Crew on the vessel below looked skywards and wondered what was going on. Johansen felt the joystick go dead in his hand. The container was released midair, falling without warning with devastating effect. Two union members were killed instantly and another was severely injured. The controls and lights in Johansen's cabin went black as he peered down at the carnage and chaos below.

Within moments, two additional cranes malfunctioned, dropping containers, damaging cargo, and killing workers before all operations were suspended. The port came to a standstill.

Emergency service vehicles arrived quickly, followed closely by journalists, camera crews, and curious and concerned onlookers. Everyone was asking what happened. On arriving, the shift manager was stopped by a journalist and speculated that there might have been a cyber attack. Another worker suggested that operator fatigue could have been a factor – "everyone's been pulling extra shifts".

An hour later, Scarn, while on holidays, and a few other leaders at Port of Nirvana received an email from the known hacker group Red Skies. It was an extortion email. Red Skies claimed it has infiltrated the port's systems. It also claimed to have taken over manifests, payroll, and purchasing data, and threaten to cause more accidents and alter data irrevocably if they were not paid USD500,000 in bitcoin. Upping the pressure, it threatened to share "sensitive and damning" information with the international media should their demands not be met.

Red Skies ended the email with "Thank you for carrying our virus and pushing it out further across the globe than we ever could have on our own."

Port of Nirvana's crisis leader and team were about to decide whether or not to pay the ransom when Red Skies sent another email, showing screenshots of the types of data they had access to. Red Skies had upped the demand to USD1 million in bitcoin. It also shared a link to where the group has some of the manifests, contracts, bank accounts, and routing numbers for sale on the dark web. Data files were being sold in batches, and it looked like 20 batches have already been purchased. Red Skies had also posted emails allegedly from employees expressing long-standing concerns about the port not having controls and processes in place to manage such events. International news outlets were reporting on the breach, social media volume swelled, and stakeholders – from clients to regulatory bodies – started to voice concern. Union protestors were assembling in large numbers at the port.

> "The communications lead is a key member of a crisis management team"
>
> **Devin Sirmenis**
>
> *Managing director of Corporate Resilience, Witt O'Brien's*

Witt O'Brien's: 5140498

Take action

What steps should Port of Nirvana's crisis management team take? What does success look like at the end of the crisis for Port of Nirvana? What workstreams have been defined? Who owns them?

Every port should have a senior-level, all-hazards crisis management plan that lays out the answers to these questions. Primary roles should be defined for positions like crisis leader, deputy, corporate communications, and functional team members i.e., legal, human resources, information technology, etc.

Each role should have a defined alternate in case the primary is not available, and the crisis extends across days, weeks, or months. Critically, the plan should match Port of Nirvana's corporate culture and be based upon how the leadership would naturally assemble as a team.

Public and stakeholder perceptions will form and solidify quickly. The best time to protect reputations is immediately. Can you issue an initial holding statement within 90 minutes for both internal and external audiences? By doing so, the port will establish that it is gripping the situation, but to respond this quickly, the port must have templates and pre-approved messaging ready to deploy.

Port of Nirvana's crisis management team should have an analysis and decision-making model built into its crisis management process. This will help structure the team's initial, as well as subsequent meetings, as the team defines and revisits the scope, size, and complexity of the current event. Scenario planning should be used to help frame what the event could become in the short, medium, and long term and what the true impacts could be on the brand and reputation of the port – its very licence to operate is threatened. Once the analysis is conducted, the crisis leader should shape the strategy, what is commonly referred to as the commander's intent – simple, visionary statements of what success looks like after the crisis. Workstreams and actions are mapped out to accomplish the strategy.

Reputation and communications objectives must be a key consideration in the strategy's development. The communications lead is a key member of the crisis management team. Especially in the early stages of a crisis, words can speak louder than actions – without communication, the company may not be seen to be effectively managing the situation regardless of what they are actually doing.

Crisis management, following actions and communications as well as managing perceptions need to be lashed together to manage the consequences of an event. PH

Be prepared

Imagine you are in the same situation as Port of Nirvana. Consider the following things:

- Does your port have a corporate-level crisis management plan with structures that convene as the crisis management team?
- If so, are the roles and responsibilities defined across the team?
- Does a small triage team meet first to determine the possible impacts of the event and call it a crisis? Or does everyone assemble at once?