Scenario

# Pen testing shows that Torvik Industries' cybersecurity breach by "The Wolf" could have been stopped by HP printers

## Official wrap-up report for the data breach

**Industry**
Shipping

**Objective**
Analyse and resolve areas of network vulnerability

**Approach**
Penetration testing to find the vulnerabilities that led to the attack

**Findings and recommendations**
- Educate users to be wary of opening suspicious emails and printing attachments
- Deploy HP printers with threat detection
- Configure all endpoints for security, including infrastructure that's moved or in temporary locations

**Business matters**
Apply stronger security measures to avoid operational downtime and improve brand confidence. Improve policies for monitoring network endpoints in temporary locations.

## Overview

Torvik Industries* ships 8 million containers each year. For 22,000 manufacturers and wholesalers, Torvik is the vital connection between products and people around the globe. Company holdings include shipping yards, vessels, warehouses, and all the technology that supports Torvik's far-flung network.

As the company has grown, its technology infrastructure has struggled to adapt. While IT security staff have configured the company's servers, some printers at satellite offices or temporary locations are not managed for security.

On April 23, 2018, the cyberterrorist known only as "The Wolf" used an unsecured printer to sabotage Torvik Industries' operations, from PCs to cranes to container ships. Their security advisor used penetration testing to analyse the event and provided recommendations for increasing security and staff training.

## What happened

Torvik Industries leadership was used to calling the shots in high-stakes games—so they didn't expect hackers to infiltrate their network so deeply that they could shut down the company's gantry cranes and redirect ships out on the open ocean.

All The Wolf had to do was compromise a large-format printer at a construction site. Then he could move laterally through the company's network to the big targets in company operations. In an instant, this top shipping company faced massive operational disruptions, intense international scrutiny, and thousands of furious customers.

## How it happened

The company's IT security staff thought they were protected. Their tech and logistical teams constantly monitored global operations for potential security problems. They even had security procedures in place for endpoints like printers. But they overlooked something: the security configuration of a large-format printer temporarily stationed in a construction trailer.

The hacker didn't even have to access the printer directly—he simply sent an email with a PDF attachment to the Torvik employee responsible for printing large-format documents. That PDF was carrying a hidden weaponised Postscript file, which could open and run itself when the PDF was sent to the printer. Once the employee sent the print job, the malware embedded itself in the printer, and then spread throughout the network. By piggybacking malware on an innocent-looking email attachment, the hacker bypassed the anti-malware software on the company PCs.

The breach was possible because the large-format printer didn't have strong built-in security, such as threat detection. Also, the company failed to monitor and manage the configuration of every single printer across the fleet—like those placed temporarily in satellite offices.

## Repairing the breach

Torvik Industries retained a top penetration testing firm to perform a thorough analysis of the organisation's cybersecurity.

The pen testing team recommended installing HP printers with embedded security features, including the HP DesignJet series with Secure Boot and firmware whitelisting. These features help the printer detect malicious code and shut down, then alert IT to the need to reinstall legitimate HP firmware.

They also recommended using the Instant-On security feature of HP JetAdvantage Security Manager, a fleet-wide security management software programme, to automatically apply security policies as soon as devices are added to the network. HP Security Manager can also create compliance reports that show every HP printer, even in remote or temporary locations. This helps demonstrate that fleet security configurations have been maintained.

In addition, the security advisor suggested an education programme to help employees recognise suspicious emails and avoid printing unknown attachments.

## Conclusion

Torvik Industries is still reeling from the impacts of the cybersecurity breach on operations, as well as heightened publicity of their president's unconventional views and criminal acts. While the organisation seeks to develop a new direction in leadership, the direction for cybersecurity is clear: turning to HP printers and solutions will help foil the next Wolf that comes hunting.

**Torvik Industries is a fictional company targeted in a large cyberattack in HP Studio's film, "THE WOLF: TRUE ALPHA."*

**For more information on HP solutions:**
HP DesignJet: hp.com/go/designjetsecurity
Print security: hp.com/go/reinventsecurity

**To view "The Wolf" films, visit:**
hp.com/thewolf

Sign up for updates
hp.com/go/getupdated

Share with colleagues



4AA7-3562EEP, October 2018