Cyberattack Setbacks Lead to Process Refinements, Renewed Precautions at Seattle-Tacoma Int'l

BY CHRIS JONES

FACTS&FIGURES

Project: Cyberattack Recovery & Resilience Efforts

Location: Seattle-Tacoma Int'l Airport, in WA

Airport Owner: Port of Seattle

Timeframe: August 2024 – ongoing

Outside Support: Check Point Software Technologies; Mandiant; Microsoft

Post-Attack Changes: Adding Information Technology staff; expediting system improvement projects; implementing 24/7 Managed Detection & Response tools from Check Point Software Technologies; reemphasizing password updates & other user precautions; more rigorous data segmentation; renewed focus on tech contingency plans for all departments

2024 Passenger Volume: 52.64 million

There will be no celebratory ribbon cuttings, no glistening new physical edifice that commemorates their work overcoming an extremely disruptive operational crisis. But even without such fanfare, team members at the Port of Seattle still knowingly appreciate their organization's recent push to restore operations and empower future resilience at Seattle-Tacoma International Airport (SEA) after a crippling cyberattack that began in August 2024.

"We used the description 'Build Back Better,'" says Matt Breed, chief information officer for the Port of Seattle, which owns and operates SEA. "Our focus was on rearchitecting while restoring, to make sure that this would not happen again by fixing the issues that caused us to get into what we got into."


MATT BREED

What the Port "got into" was one of the highest-profile cyberattacks in history. In the days that immediately followed, hordes of travelers at the nation's 12th-busiest passenger airport temporarily went without the convenience of printed baggage tags or check-in kiosks. There was no Wi-Fi service or digital information

displays to provide expected details on arrivals, departures or baggage claim carousel assignments.

Without the usual Wi-Fi service, travelers jumped onto SEA's distributed antenna systems while trying to use cellphones for internet access. That overwhelmed nearby cellular networks and forced the need for delivery of outside equipment to keep everyone connected.

Online reserved parking, the SEA Spot Saver security checkpoint virtual queue and the Port's website were knocked offline for travelers, and staff members were unable to access essential workplace systems such as email and network storage drives. Communicating with the public became arduous, and many passengers found themselves almost entirely reliant on printed signage or face-to-face interactions with staff to continue their journeys.

To make matters worse, Port leadership understood there was no quick fix available. Hackers had encrypted core data files and demanded a large ransom payment to secure their release. The Port was unwilling to meet those demands, but also knew rebooting the system would not be sufficient. A full rebuild was necessary—and that would take months to fully complete.


STEPHANIE WARREN

"It was an incredibly easy decision from an information security perspective, but not a business perspective," recalls Stephanie Warren, assistant director of Information Security for the Port. "There was activity on that server, and looking at how long they'd been in our backups, (the implication was) we were not bringing anything in that environment back.

"So we rebuilt the data center from scratch."

Along the way, tech-centric challenges unintentionally presented opportunities to highlight and further refine the Port's strategies for public communications and customer service. Can-do frontline workers who rose to the occasion now carry forward a legacy of service that coalesced right before travelers' eyes during the recovery phase.

Warning Signs

In the early hours of Friday, Aug. 23, 2024, Port cybersecurity staff members came across a single alert that raised red flags. The more they investigated, the more worrisome their steady discoveries became. A daylong review spilled over into early Saturday, and around 1 a.m., a staff member detected hackers working inside the Port's servers at that very moment.

The airport scrambled to supply flight information while digital systems were down.

Warren describes the scene that followed as something out of a television drama, with colleagues bellowing, *"I need this!"* and issuing urgent orders to head off attackers who were later identified as members of Rhysida, a global cybercriminal network. "We were trying defensive maneuvers, and it became very clear that they were beginning to add more bodies and seats to outnumber us," she recalls. "They had people sitting at keyboards actively going back and forth with us."

As the Port's cybersecurity team realized the attackers weren't just automated bots that could be fended off easily, it began methodically shutting down systems in a rapid-fire manner.

That process took less than an hour and was immediately followed by further triage assessments and alerts to Port leadership. But from that point forward, no data could move in or get out to staff, tenants or customers. The Port's local network and auxiliary data center located across the state near Spokane were effectively transformed from two-way communication pathways into "digital islands," Warren notes.

The Port's overall information technology network relies on two common systems: operational technology, which monitors and controls automated devices, processes and infrastructure; and enterprise software, which supports primary business processes such as email, file sharing and other user-focused functions. An after-incident investigation revealed that Rhysida hackers penetrated the Port's enterprise network months earlier via a worker's infected laptop, and from there proceeded to compromise the operational technology.

In retrospect, it appears the cybercriminals were patient and nimble. Details gathered suggest that the attack was originally planned for a week later, when more Port staff would be away over the extended Labor Day weekend. Instead, the hackers were rushed into action early when staff detected their digital presence on Aug. 23.

Without that pivotal catch, the situation could have been much, much worse for SEA and its users.

"We saw partial execution of the encryption," Breed explains. "They should have shut our servers down and encrypted them right away. They didn't do that."

Fortunately, the attack's effects were also limited in several important facets, most notably safety and security. Federal agencies such as the TSA, FAA and U.S. Customs and Border Protection were unscathed because each maintains its own proprietary systems at SEA.

The airport's larger airlines—including Alaska and Delta, which together accounted for 76% of SEA passenger volume in 2024—were likewise less affected. They continued operating in a

GateKeeper Systems
OPTIMIZED SOFTWARE SOLUTIONS FOR AIRPORTS
GateKeeper App-139
Automate all Inspections and Work Orders!
FAA Inspection Compliance!
SMS and training module!
GateKeeper TNC-Ops
Compliance enforcement!
Validate monthly TNC revenue!
Now featuring access control via LPR cameras!
GateKeeper CVMS
Flexible & affordable off-the-shelf software!
Streamline administrative operations!
Virtual queueing with GateKeeper eDispatch!
651-365-0700 www.gksys.com

relatively normal manner using their own information technology networks and tools to process passengers and checked bags.

Still, Labor Day weekend was on the horizon—a peak for Seattle's Alaskan cruise season and other end-of-summer trips through SEA—and many low-cost and international carriers were suddenly unable to access the airport's common-use systems.

Puget Sound Principles

Let's pause to address a common question: Why didn't the Port simply pay Rhysida's 100 Bitcoin ransom, which was equivalent to about $6 million at the time?

The answer came down to principles and strategy.

Steve Metruck, executive director of the Port since February 2018, explains that meeting ransom demands from the cybercriminals was never an option because doing so would have violated the organization's pledge to be a good steward of taxpayer dollars. For reference, Metruck has held public roles for more than four decades, including the rank of Rear Admiral before retiring from the U.S. Coast Guard years earlier.

In addition, Rhysida is known for frequently demanding second ransom payments after victims pay the first rounds. "It would have been foolhardy," says Breed. "We had very little confidence we were going to get our systems back cleanly (through payment)."

Yet even with the attackers shut out and effectively cast aside, the challenges at SEA remained formidable.

The path forward began by first determining *how* to recover. Using primary backups was impossible since hackers had sufficient time to compromise those systems. Some of the backup files had even been deleted altogether, including many from the Port's auxiliary data center.

All available internal resources were marshalled to devise the best strategy. In addition, the Port turned to outside contacts at Microsoft, which is headquartered just a few miles from SEA, and Check Point Software Technologies, a global cyber security firm based in Tel Aviv. Their respective teams focused on finding and removing the hackers' work. Google-owned Mandiant, a leader in dynamic cyber defense, threat intelligence and incident response services, also provided assistance in conjunction with Microsoft.

While SEA was still navigating the ripple effects of the attack, Breed recalls Microsoft Chief Executive Officer Satya Nadella indicating that it was a top priority for the company to support its hometown airport.

Managing the Message

Technology troubles notwithstanding, determining what to say about the incident and when to say it added even more challenges.


CHRIS GUIZLO

Chris Guizlo, the Port's director of External Relations and Communications, was SEA's on-call media responder the weekend of the attack. Around 3 a.m. on Aug. 24, Guizlo was alerted that systems were down and passengers had no internet access. He quickly reported to the airport where things soon went from normal to "cascading" as more outbound flights couldn't access SEA's common-use systems.

Providing updates was initially difficult due to the lack of email service, internet access and other common tools. Guizlo and team could only use their cellphones to communicate, and the system they needed to operate was overloaded by customer use due to lack of onsite Wi-Fi.


ABBEY LAMPERT

But there was one ace in the hole: Social Media Program Manager Abbey Lampert was logged into the Port's and SEA's social media channels from her home, where she had functional Wi-Fi.

"We used that as our vehicle to get our updates out," Guizlo explains, adding that local media had previously been trained to check the airport's X (nè Twitter) feed for information during big events. As cell service allowed, staff relayed information to Lampert, which she then posted on SEA's social platforms for the general public.

Prior training on the National Incident Management System (NIMS) made the Port's communications crew comfortable working closely with the event's incident commander using an Emergency Operations Center setup. The team's first-day messaging focused on the customer impact, noting which airlines were or were not affected, providing information about TSA checkpoint lines and affirming that shops and restaurants were still open.

The situation became more critical on Sunday due to a heavier schedule of international arrivals. These carriers, which use common-use systems, had lost their ability to electronically check in passengers or to print tags for checked baggage. Delays ensued immediately.

Aviation Managing Director Lance Lyttle, then SEA's top official, held a press conference that afternoon alongside local TSA and Customs and Border Protection leaders. Each stressed that safety and security were not compromised by the incident and acknowledged that there would be temporary inconveniences.

"That took down the temperature quite a bit," Guizlo recalls.

Still, he and his communications team walked a fine line over the next few days. They needed to provide travelers with important information without sparking speculation into what had caused SEA's problems. Admitting there was a cyberattack prematurely would have affected the ongoing investigation, and perhaps encouraged other bad actors to strike similarly, Breed explains.

It wasn't until Sept. 13—nearly three weeks later—that the Port publicly confirmed an intense examination had concluded the outages were "consistent with a cyberattack."

"People (then) gave us a little bit of understanding because they've seen that happen to other organizations," says Guizlo of the eventual public acknowledgement.

Where to Start?

Prioritizing functions was paramount during the recovery effort, with longer-term items being set aside for operational needs, as directed by executive management. Although the Port had continuity of operations plans (COOPs) already in place, implementing them revealed some big surprises.

Printers emerged as an unexpected core need, particularly to create signage for travelers while most of the digital displays were not functional. "Being able to print was huge, and the fact that the organization was so dependent on that was shocking, in retrospect," Breed notes.

Limited access to anticipated response tools was another shortcoming. Because the Port's active directory was dumped, most staff couldn't access Microsoft 365 or other everyday applications. Nearly 2,500 workstations were upgraded to Windows 11 after they were encrypted. Software was painstakingly reset with new passwords and logins, requiring significant time to coordinate between information technology staff and affected employees.

Once the decision to rebuild the data center was made, Port staff used available hardware that had been previously purchased for other upcoming projects. Coupled with new orders facilitated by trusted reseller World Wide Technology, a new data center began to rise from the ashes. An outside data infrastructure company provided further support through its storage and cloud-based tools.

There was a near-daily balancing act, however, as immediate operational needs conflicted with informational technology security. Despite that, Warren says stakeholders remained incredibly collaborative to ensure no system came back online prematurely.

"It was a constant back and forth of finding new information and then figuring out how we can bring something back safely," she says. "From a (security) perspective, I was 'Burn it to the ground and rebuild,' even though I know that was never really an option."

Good fortune reared its beautiful head once again thanks to a Port server engineer who, before the attack, was preparing to run tests on new file server hardware. In the course of that work, she had placed weekly copies of data in a legacy location that was unknown to and remained uncompromised by Rhysida.

"That was where we ultimately recovered our saved data," Warren says.

Even so, that stroke of luck revealed a shortcoming that needed to be corrected going forward. Those copied files, Breed notes, never should have existed in a legacy location outside of the Port's newer cloud-based SharePoint systems that remained protected from the hackers' breach attempts.

"It became very apparent that a lot more people were using that legacy file share than we had estimated," he says. Campaigns strongly encouraging Port staff onto the cloud are now continually emphasized to help lessen the likelihood of future data vulnerabilities.

Turning the Tide

Port leaders report that SEA received strong support from its airlines and internal stakeholders, with most frustrations stemming from uncertainty about when tech systems would come back online. Despite disruptions to vital processing systems, the airport experienced some delays but no flight cancellations.

"I'm amazed that we kept chugging along," Breed says.

Staff hand wrote baggage tags Aug. 24 to 25, and then used generic printed tags until the Port could access uncompromised backup files to restore its normal processes. Once achieved, that crucial milestone also re-enabled common-use carriers to check in passengers electronically.

Public communications duties were divided into three functional areas. Guizlo served as the overall lead, with Media Relations Manager Perry Cooper handling press inquiries, and Lampert leading the social push. They all recognized the power of imagery and tasked any staffer with a smart phone to capture and send them videos and still photos.

If an employee spotted a blacked-out display, for example, that imagery was shared via social media. The same applied as travelers were observed waiting in long lines at baggage claim, or when staff offered directions with hand-written signs.

"I needed those pictures to tell that story for media, as well as for the public," Guizlo explains. "We can say it over and over again, but being able to see it is a different story."

Guizlo credits trust between his team and Port leadership, which set up basic guardrails but otherwise did not interfere with efforts to provide transparency. This allowed them to fend off rumors and address issues before they grew into crises.

Since many members of the Communications team have journalism backgrounds, they were able to anticipate which

IMPACT RECOVERY™

SlowStop® Protective Guarding
Protect What Keeps Airports Moving

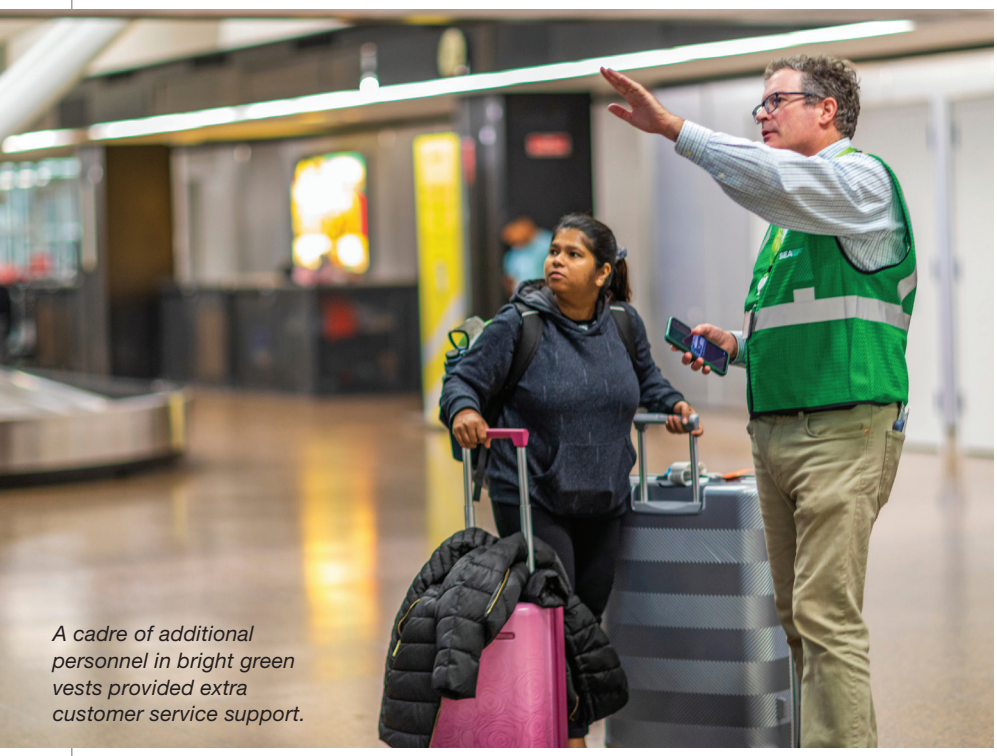
Rebounding Steel Barriers Trusted at Airports Worldwide

SlowStop® Protective Guarding delivers reliable, rebounding steel protection designed for the unique demands of airport environments.

- *Shields baggage areas and ground support equipment*
- *Guards gates and airside operations from vehicle strikes*
- *Improves passenger and employee safety*
- *Prevents costly repairs and downtime*

Scan to Learn More

impactrecovery.com • 1-800-736-5256 • 4955 Stout Drive • San Antonio, TX 78219



A cadre of additional personnel in bright green vests provided extra customer service support.

questions were likely coming and determine how best to answer them. Cooper also repeatedly took time to walk members of the press around the airport for first-hand understanding.

"I told (leadership) we needed to be posting updates twice a day," Guizlo says. This approach built what he calls an "amazingly effective strategy" for public confidence.

Green Cavalry

Just when it was needed, help began pouring in from unexpected places. Port staff from facilities across the region, including seaports, volunteered in large numbers to assist air travelers. Julie Collins, director of Customer Experience and Brand at SEA, deftly dubbed these eager helpers the "Team in Green" after the bright vests they wore while providing key customer support with a friendly smile, even when directing guests to the nearest restrooms over and over again.

EZLINER®
Proven, Reliable, Cost-Effective
SCAN FOR ADDITIONAL INFORMATION

Paint equipment built to optimize time, money, and safety.

BENEFITS:
- Marks up to 36" wide in a single pass
- Accommodate multiple additional guns to be able to paint patterns and colors in a single pass
- Exclusive use of latex paint, creating less runway debris

Sourcewell Awarded Contract

EZLINER - ARROW | (800) 373-4016 | ezlinerarrow.com | sales@ezlinerarrow.com | Billings, Montana | Orange City, Iowa

canoe APPROVED SUPPLIER

"It was honestly one of the biggest morale boosters internally because they felt like they could help, even if they couldn't do their regular jobs," recalls Guizlo.

By Wednesday, Aug. 28, processes in the terminal had normalized enough that the Communications team could shift from assuaging fears over disruptions to addressing the upcoming Labor Day passenger surge. Issuing travel tips during that period is an annual tradition, but SEA took a different approach in 2024 by having staff members share the information in social media videos.

Showing the faces of those who had worked so hard to lend assistance humanized the Port's challenges in a favorable manner, Guizlo explains. It also boosted morale among employees who felt their extra efforts were being appreciated and highlighted. The videos reinforced the message that most flights and services at SEA were no longer affected by the cyberattack. "It was really getting into the nitty, gritty details of who's going to be impacted by what," Lampert says.

As systems came back, each win was widely shared and celebrated. Local social media influencers even got into the act unprompted, praising Port staff for working so hard to keep travelers informed and moving with few interruptions.

"Being able to show people that we're here, we're listening, we're trying to get you the information we can give you just shows them that we're understanding and we get it," Lampert says. "That went a long, long way with all of our customers."

Lessons Learned—and Shared

Now more than a year later, Warren says there is only one absolute takeaway from the attack: Airports will never be 100% immune to vulnerabilities, no matter how hard they try.

But that doesn't mean organizations should stand by idly while hackers across the globe scheme new and innovative ways to crack their defenses. Breed likes to remind his industry peers that the damage caused by cyberattacks outnumbers by "orders of magnitude" how little is spent on cybersecurity. To flip that script, SEA is increasing its information technology staff and expediting system improvements rather than "kicking the can."

Among the positive changes prompted by the 2024 attack, Breed cites the addition of 24/7 Managed Detection and Response tools.

"I.T. departments are often understaffed and…changes can be disruptive and difficult to complete. But there's no tolerance for cutting corners anymore," he reflects. The Port quickly completed two to three years of previously stalled projects in the aftermath of the attack because it became imperative that those improvements no longer be delayed, he adds.

Counter personnel used manual workarounds to continue processing passengers.

There were also cultural changes such as reminding colleagues why cybersecurity training, however annoying it may be—is, in fact, necessary.

"There is a balance between security and operations, but now the pendulum has swung much more toward the security side," Breed comments. "It's something we have to remain focused on for the long term. It's a continuous arms race with these threat actors."

Working with Microsoft and others, the Port has become much more rigid about segmenting data to make it more difficult for hackers to jump from one network area to another. Users are now denied direct access to servers and must pass through virtual private networks that determine who is accessing the system, and from where.

Well-exercised contingency plans are the new standard across *all* Port departments, Warren reports. Some units performed well, while others less so, in 2024. Going forward, the goal is for each unit to create and understand its own unique resiliency plans for any type of disruption. This includes diligent efforts to prioritize tasks and identify mission-essential needs—even for easily overlooked details such as printers.

"When you talk about cyber, people automatically respond, 'That doesn't involve me. I don't deal with computers,'" Warren says. "But it does, because any technology disruption means an operational disruption."

Those who suggest the Port's policies left it vulnerable to an attack are mistaken, Breed adds. Instead, he cites a convergence of circumstances that began with an infected device and software tools that failed to remove all bad files. Rather than being wiped 100% clean, that laptop was somehow reconnected to the network where hackers were then able to spread beyond that device, largely unnoticed. Among Breed's key takeaways: Don't just assume your defenses are working as planned and never overlook the small stuff.

"A lot of the triggers that were seen were (initially) seen as individual events that we had already cleaned up," he explains. "The big picture did not emerge until this full attack."

As airport functions normalized, Lampert recalls realizing that the Port's communications strategy also couldn't simply snap back into pre-attack work patterns. "You can't just pretend everything's OK; we had to answer the elephant in the room," she comments.

Restoring the Port's website in time for Thanksgiving travel was a key priority that took several more weeks. During that time, messaging temporarily continued over longform blog entries on LinkedIn and Facebook. These often featured interviews with employees to further highlight SEA's well-received "Team in Green" theme.

"To the public, things were better at the airport. But our systems were still affected internally," Lampert describes. "It wasn't a black and white switch. There was that really good gray area before we could pivot."

As 2024 fades further into memory, Port representatives hope sharing their experiences will assist other airports and organizations to avoid similar predicaments. "We wanted our sad story to be a lesson instead of others having their own sad stories," Warren remarks. "Airports are now forming a united front to make us stronger as an industry."

To that end, Breed was recently contacted by staff from two other airports who said they had warded off cyberattacks thanks in part to lessons SEA had shared.

"(Transparency) helps us get stronger as an industry," he concludes.