41st Annual AAAE
Airport Law Workshop
Washington, D.C.

Session #11

Airport Cyber Attacks: The Role of the Legal Advisor

KAPLAN KIRSCH

AAAE

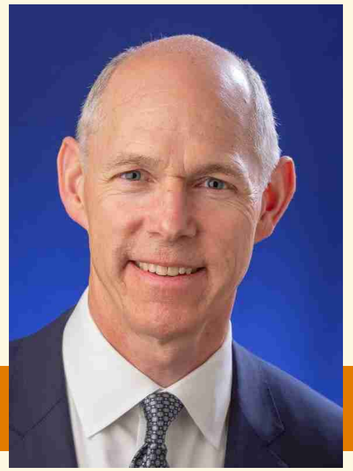
IMLA

Speakers

Jessica Nadelman

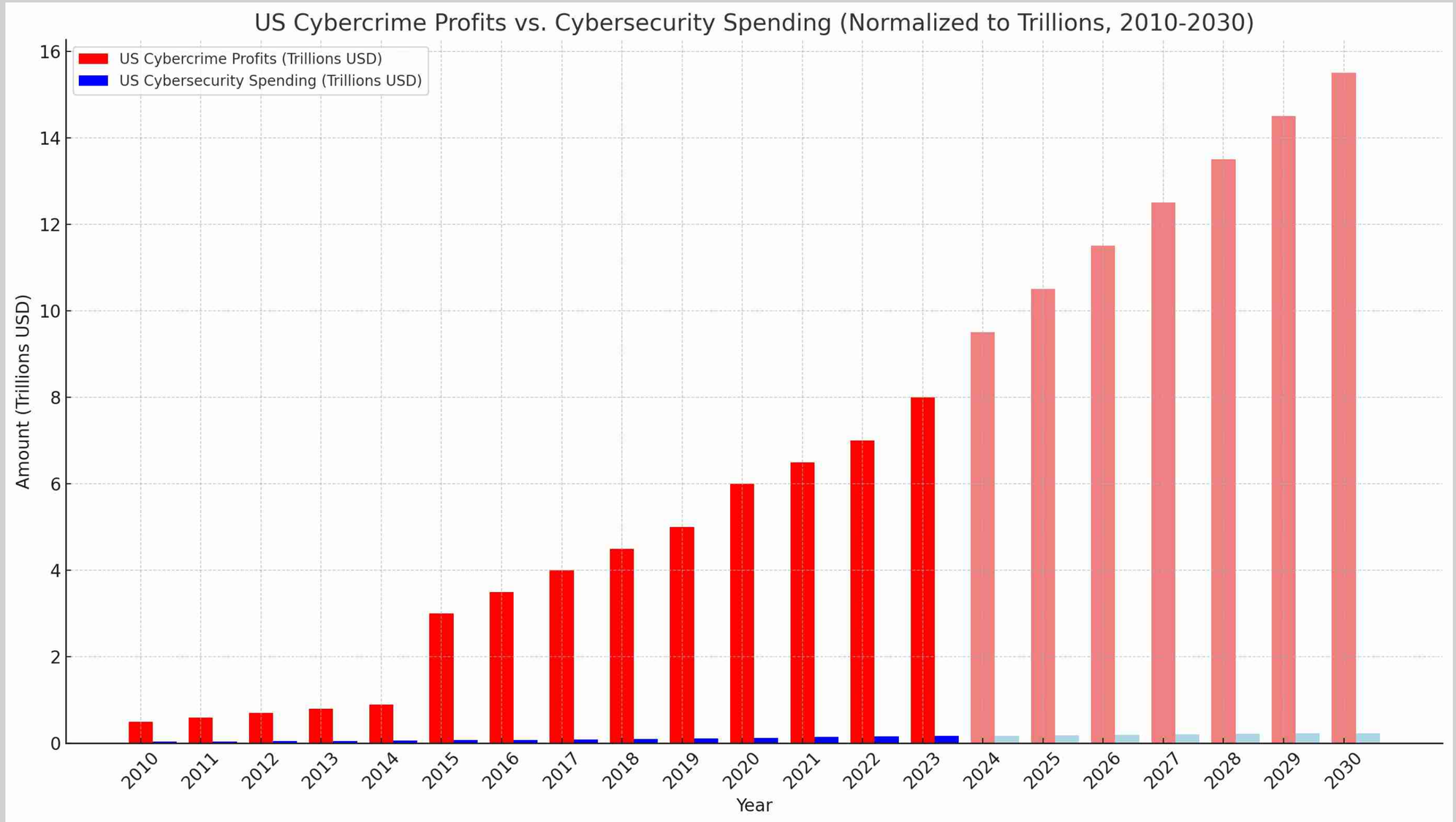
Senior Port Counsel
Port of Seattle

Pete Ramels



General Counsel
Port of Seattle

Critical impact



The role of the legal advisor - overview

Cyber attack timeline

July 2024
Rhysida
Ransomware used to attack the Port

July to August 2024
Lateral movement
Privilege escalation
Network recon
Staging attack points

August 2024
Data exfiltration
System encryption
Port of Seattle network lock down & isolation

The role of the legal advisor - cyber attack initiation

Customer disruptions

Free Wi-Fi

Digital

Website
Mobile Apps
TSA Wait Times

Systems

Parking
Secure doors
Alarms
Baggage

Displays

Arrivals
Departure
Baggage

Common Use

Organizational disruptions

Network

Wi-Fi

Desk Phones

Office365

Email

Teams

SharePoint

Port-Wide Comms

Business Functions

Payroll

Contracts

Accounting

Badging

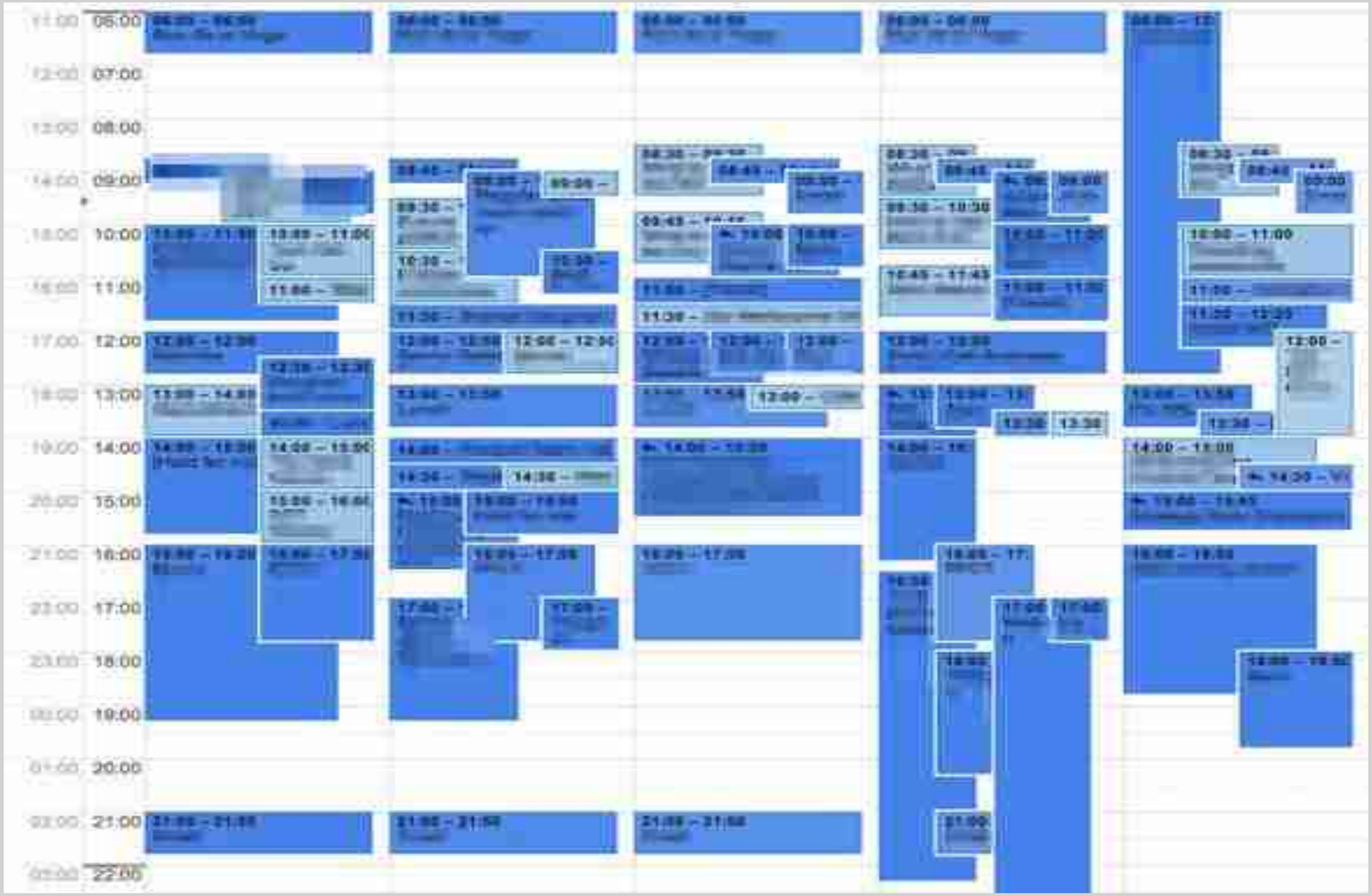
Printers

Scanning

Faxing


AIR TAHITI NUI
CONDOR
HAINAN AIRLINES
VOLARIS
AER LINGUS
ANA
BRITISH AIRWAYS
EVA AIR
HAWAIIAN AIRLINES
JAPAN AIRLINES
QATAR AIRWAYS
SEA

The role of the legal advisor - crisis response



The role of the legal advisor - crisis response

- Contracting
- Compliance
- Communication
- Coordination and Consistency

Ransomware payment demand

“From day one, the Port prioritized safe, secure and efficient operations at our facilities. We are continuing to make progress on restoring our systems. The Port of Seattle has no intent of paying the perpetrators behind the cyberattack on our network. Paying the criminal organization would not reflect Port values or our pledge to be a good steward of taxpayer dollars. We continue working with our partners to not just restore our systems but build a more resilient Port for the future. Following our response efforts, we also commit to using this experience to strengthen our security and operations, as well as sharing information to help protect businesses, critical infrastructure and the public.”

Steve Metruck, Executive Director

Threat actor – data release

The role of the legal advisor - threat actor/ransom

- Engage vendor
- Ransom payment decisions/policy
- Balancing/explaining risks to organization
- Federal law enforcement engagement
- Communication strategy
- Employee concern - credit monitoring

Recovery

Detection, Investigation, and Recovery

Continuity of Operations

Communication

Regulatory oversight and information sharing

The role of the legal advisor - recovery

Balance competing priorities:

- Forensics vs. restoration
- Security risks
- Operational needs
- Reputation
- Financial
- Regulatory compliance
- Convenience

The role of the legal advisor - recovery

Examples of impacts with legal significance:

- ✓ Payroll delays
- ✓ Work stoppage
- ✓ Revenue slowed
- ✓ Procurement and hiring interruptions
- ✓ Records production halted
- ✓ Website outage

Post incident - after action review

Transparency and information sharing goals

> "*We will be conducting an after-action review of this incident that will result in new information and insights*." - Senate testimony

After action review process:

- Interview key individual stakeholders
- Conduct group discussions with business units and external organizations
- Examine relevant documents, reports, logs/notes, and records
- Identify root causes and make recommendations

Organizational continuity and resiliency program

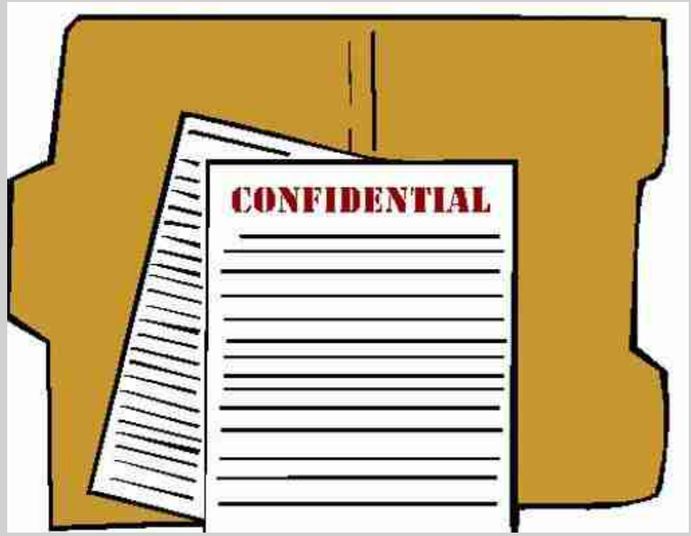
Technical Initiatives

Organizational Change

Disruption Preparedness

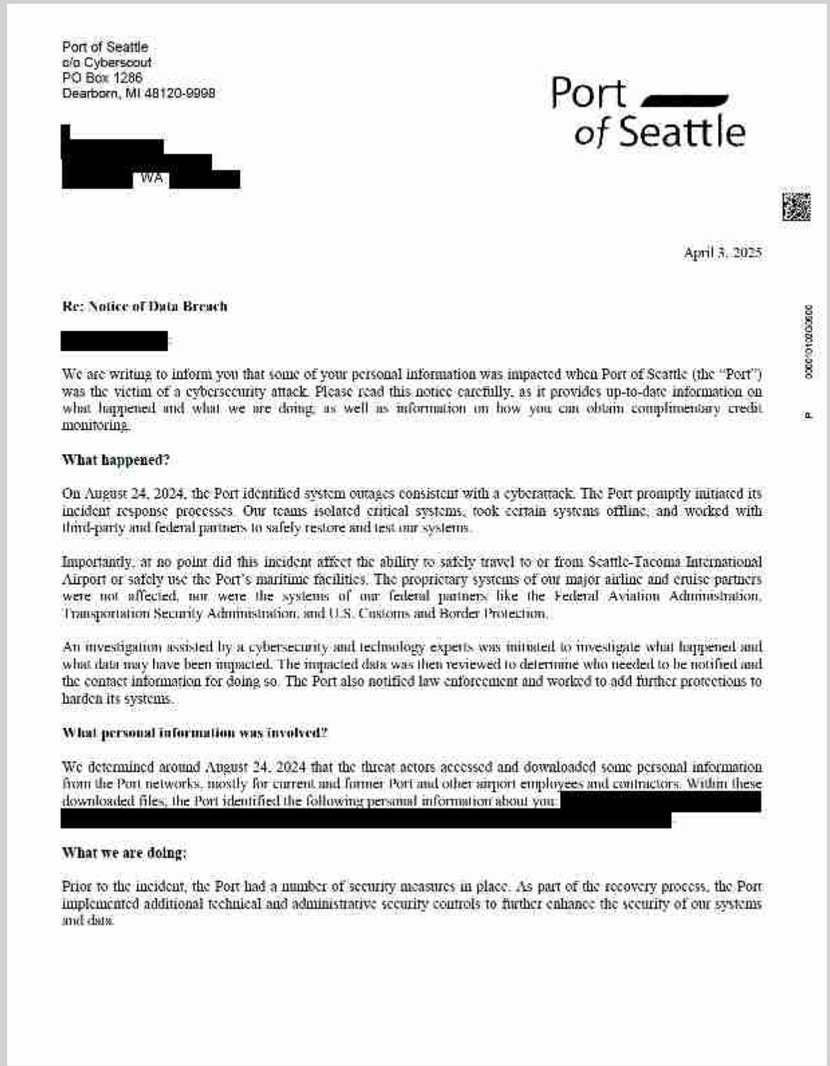
The role of the legal advisor - after action review

- Privileged engagement
- Management of process
- Transparency/risk balancing
- Guidance on recommendations



Post incident – data breach notice

- Individual notifications
- Substitute notification/media
- Attorney General notification



Port of Seattle
c/o Cybescout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]
WA

Port of Seattle

April 3, 2025

Re: Notice of Data Breach

[redacted]

We are writing to inform you that some of your personal information was impacted when Port of Seattle (the "Port") was the victim of a cybersecurity attack. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring.

What happened?

On August 24, 2024, the Port identified system outages consistent with a cyberattack. The Port promptly initiated its incident response processes. Our teams isolated critical systems, took certain systems offline, and worked with third-party and federal partners to safely restore and test our systems.

Importantly, at no point did this incident affect the ability to safely travel to or from Seattle-Tacoma International Airport or safely use the Port's maritime facilities. The proprietary systems of our major airline and cruise partners were not affected, nor were the systems of our federal partners like the Federal Aviation Administration, Transportation Security Administration, and U.S. Customs and Border Protection.

An investigation assisted by a cybersecurity and technology experts was initiated to investigate what happened and what data may have been impacted. The impacted data was then reviewed to determine who needed to be notified and the contact information for doing so. The Port also notified law enforcement and worked to add further protections to harden its systems.

What personal information was involved?

We determined around August 24, 2024 that the threat actors accessed and downloaded some personal information from the Port networks, mostly for current and former Port and other airport employees and contractors. Within these downloaded files, the Port identified the following personal information about you: [redacted]

What we are doing:

Prior to the incident, the Port had a number of security measures in place. As part of the recovery process, the Port implemented additional technical and administrative security controls to further enhance the security of our systems and data.

0000010100000

The role of the legal advisor – data breach notification process

- Data mining
- Contracting/oversight for notification vendor, credit monitoring, call center
- Review all external communications and notices
- Internal messaging
- Media briefings

Data breach litigation

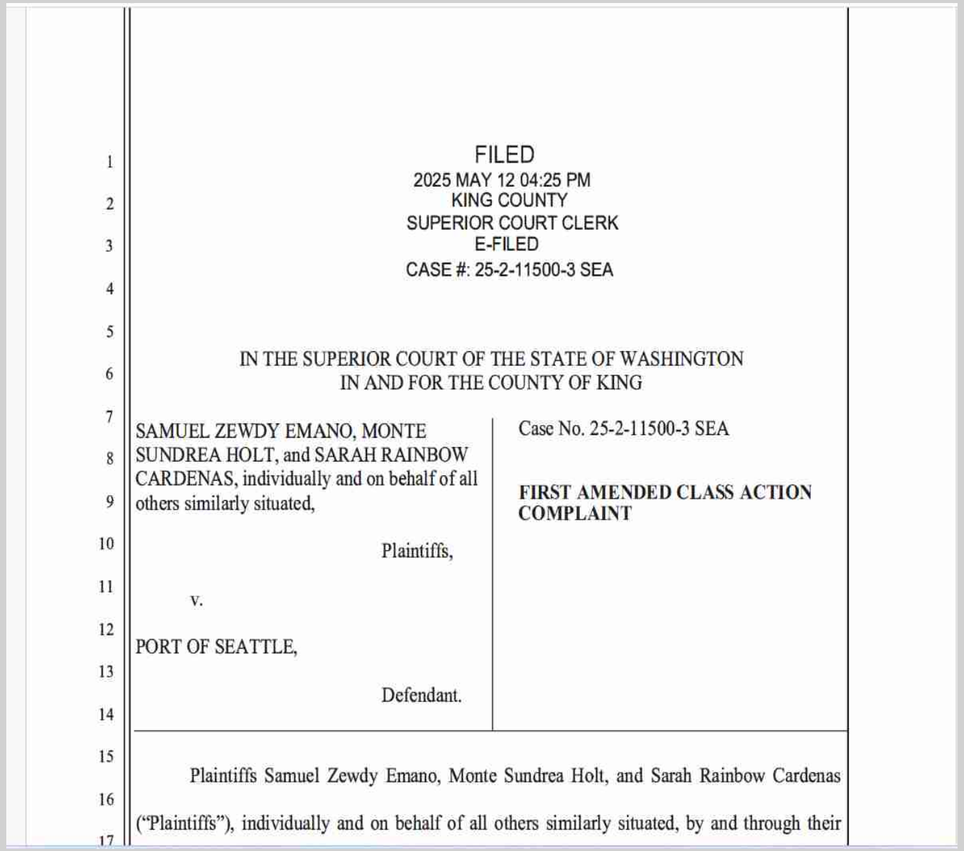
Impacted individuals

- Threshold notice volume to trigger lawsuits

Port litigation

- Four lawsuits filed
- Consolidated into class action

Media attention



FILED
2025 MAY 12 04:25 PM
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE #: 25-2-11500-3 SEA

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

SAMUEL ZEWDY EMANO, MONTE SUNDREA HOLT, and SARAH RAINBOW CARDENAS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

PORT OF SEATTLE,

Defendant.

Case No. 25-2-11500-3 SEA

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Samuel Zewdy Emano, Monte Sundrea Holt, and Sarah Rainbow Cardenas ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their

The role of the legal advisor – data breach litigation

Relevant Factors	Seemingly Irrelevant Factors*
How many individuals impacted	Measurable harm to individuals
How many plaintiff's attorneys involved	How much insurance coverage is available
How much spent on post–incident rebuild/security	Existing security measures/nature of attack
What type of data was accessed	Prior data breaches of same data
Jurisdiction of event	Current location of individuals
Age and source of data	Efforts to notify impacted individuals

Negotiated settlement amount

The role of the legal advisor - readiness

Legal and Technology Staff Partnership

Prevention

- Build relationships with tech and security staff
- Adhere to retention/disposal protocols
- Consider privacy policy
- Third party access policy/contractual security clauses
- PII storage – data mapping
- Support security budget requests – **consider security audit**

The role of the legal advisor - readiness

Legal and External Partners

Preparation

- Outside Counsel
- Established guidelines for information sharing
- Cyber insurance and preferred vendors
- Notification obligations-regulatory and contractual
- Communication channels

The role of the legal advisor - readiness

Legal and Emergency Preparedness

Response

- Incident response plans
- Escalation protocols for decision-making
- Information sharing with outside partners
- COOP’s
- Business Impact Analysis
- Recovery prioritization

41st Annual AAAE
Airport Law Workshop
Washington, D.C.

Questions?

KAPLAN KIRSCH

41st Annual AAAE
Airport Law Workshop
Washington, D.C.

Thank You!

KAPLAN KIRSCH