

2024 TLA Annual Conference & CTLA Mid-Year Meeting

May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico
Golf and Beach Resort
Rio Grande, Puerto Rico



Transportation Lawyers
Association

CTLA





May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico Golf and Beach Resort
Rio Grande, Puerto Rico



A RANSOMWARE TALE

SPOILER ALERT: THERE IS NO FAIRY TALE ENDING

The Cybersecurity Presentation Association of America Has Rated This Presentation R: As In Required Viewing For The C-suite

Justin S. Daniels

Baker Donelson

Shareholder

678.406.8706

jdaniels@bakerdonelson.com

Scott D. Carey

Shareholder

Nashville | Atlanta

615.726.7379

scarey@bakerdonelson.com

Troy M. Bettencourt

IBM X-force

Global Partner & Head

941.979.7246

troy.bettencourt@ibm.com

Christian Nieves

Supervisory Special

Agent – Cyber

FBI San Juan Division

O: 787.987.6280

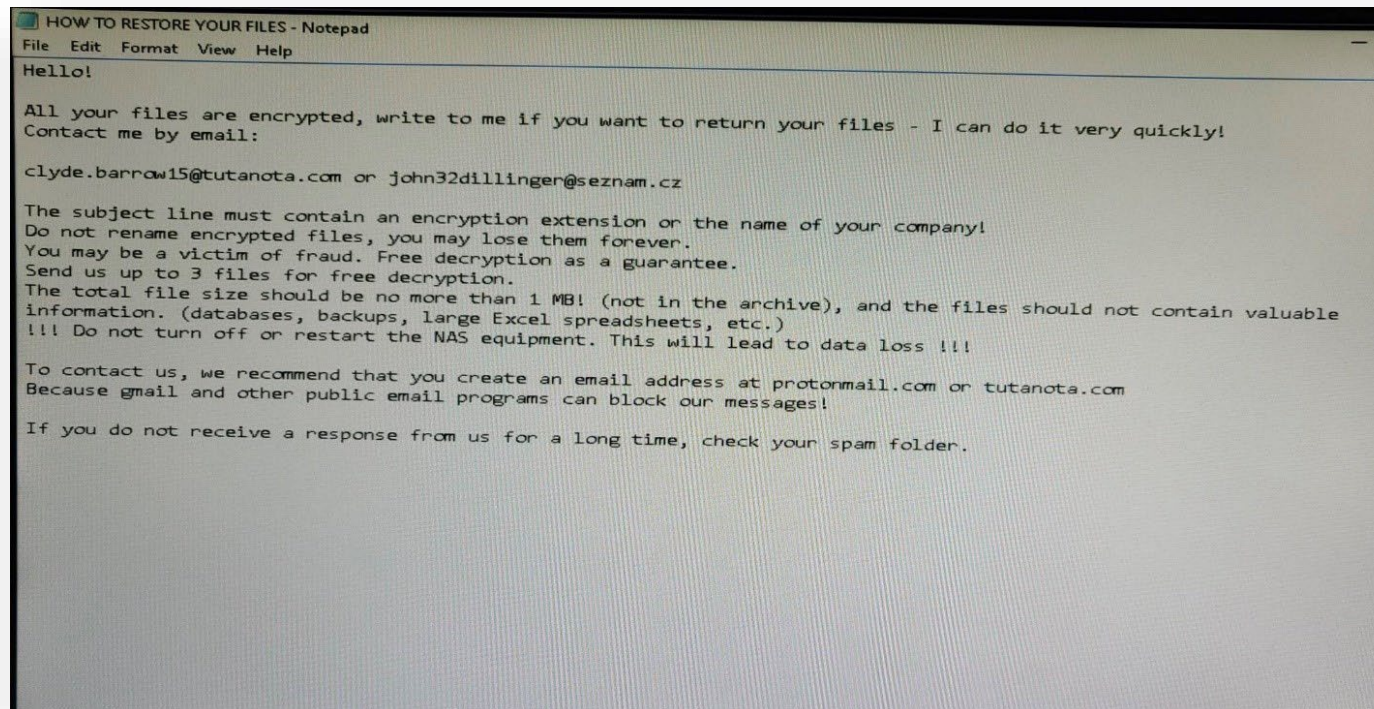
M: 787.647.9093



May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico Golf and Beach Resort
Rio Grande, Puerto Rico

A Pleasantly Sounding Unpleasant Note





What Do We Do Now?





May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico Golf and Beach Resort
Rio Grande, Puerto Rico



Breach Team

Time is precious – yet most companies don't know who to call when they are the star in the Ransomware Tale!

All hail the forensics team...what is this privilege thing?

What is a ransomware negotiator and why do I need it?

What is the comms plan?





May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico Golf and Beach Resort
Rio Grande, Puerto Rico



Customer and Employee Communications

As Crash Davis says: Learn your Cliches “network outage” “disruption to the network”

Just the facts, NO SPECULATING as this story changes hourly!

Always qualify what you say with the words “the investigation is ongoing.”

Do you have a solid NDA in case you have to discuss the cyber event with specific customers?





May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico Golf and Beach Resort
Rio Grande, Puerto Rico



Forensic Analysis: Separating the SH From the IT

How did the TA get in?

What systems were impacted?

Any evidence of data exfiltration?

Any concern of migration to customer's systems?

Any issues with the integrity of backups?

How will we get the TA out?



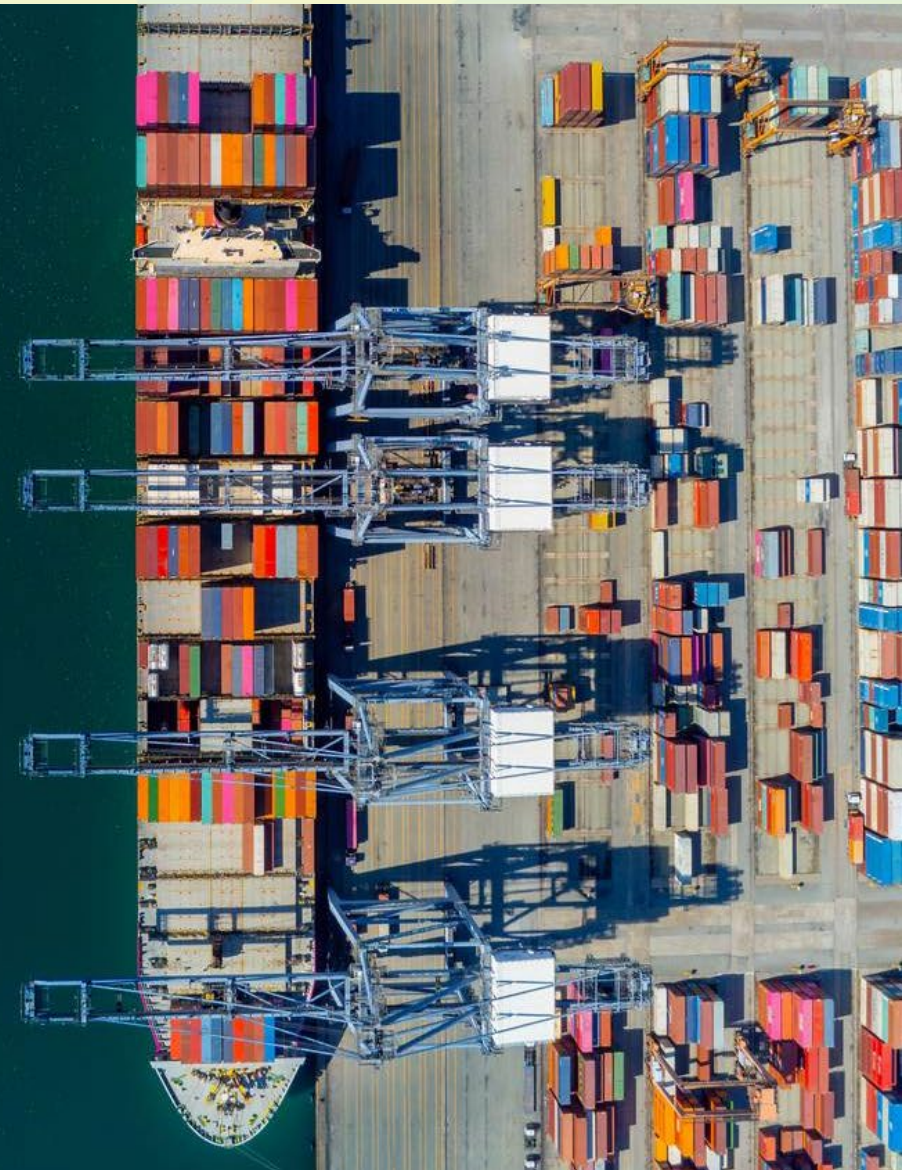
The Ransomware Negotiation Dance

Do you have to negotiate and how do you do it?

Request proof of decryption (Do not send PI/PHI files).

Do not pay the ransomware without interacting with law enforcement: Booby prize could be prosecution for aiding terrorism!

Do not assume the decryption key will work on all files.



A Pause for Privacy

Do you collect PI or PHI?

Do you store PI or PHI?

Do you process PI or PHI for others?

Do you know where it is on your network?

Will PI or PHI appear in unexpected places?

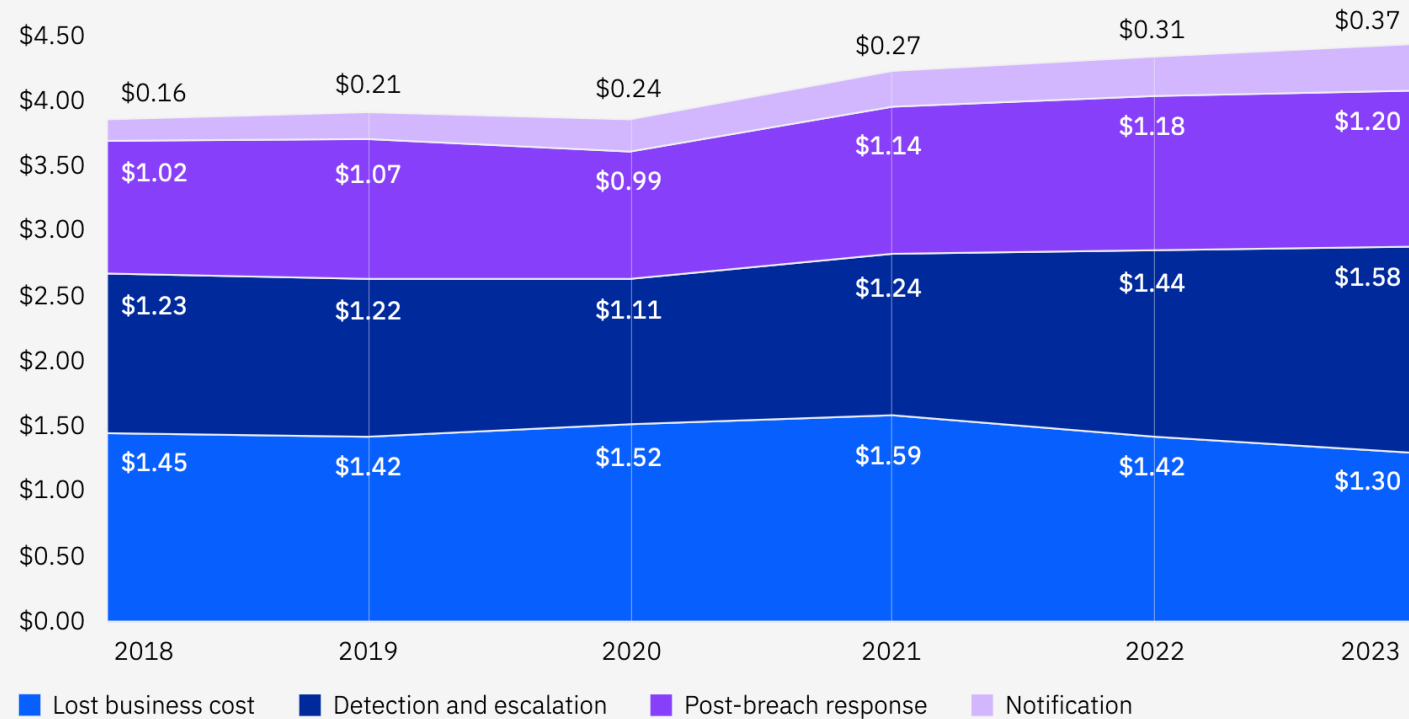
Breach Notification Rules

GDPR: 72 Hours After the Breach
VS.

50 U.S. Breach Notification Laws
(Time Period Varies by State)



Cost of a data breach divided into four cost segments



USD 4.18M

Average cost of a data breach in Transportation

8th highest cost
of 17 industries studied

6% lower than the
USD 4.45M global average

Global highlights

Top 3 initial attack vectors



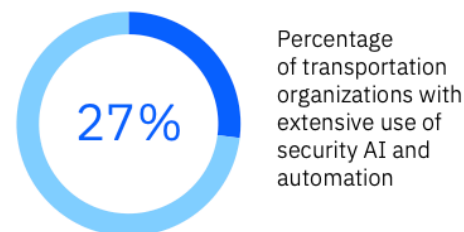
USD 332M

Average total cost of a
breach of > 50M records

USD 5M

Average cost of ransomware-
related breach

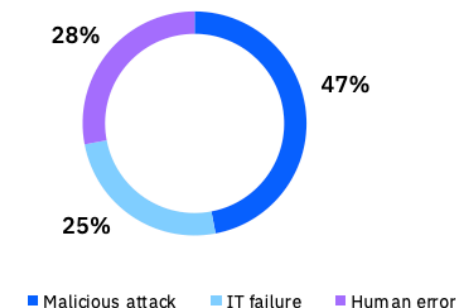
Key statistics



USD 850,000

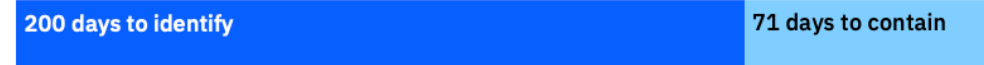
Cost savings of fully deployed security AI and automation versus global average cost of a breach

Root causes of a data breach



Time to identify and contain

Transportation industry



Global average



USD 1.5M

Average cost savings with incident response (IR) teams and testing versus no IR teams or testing

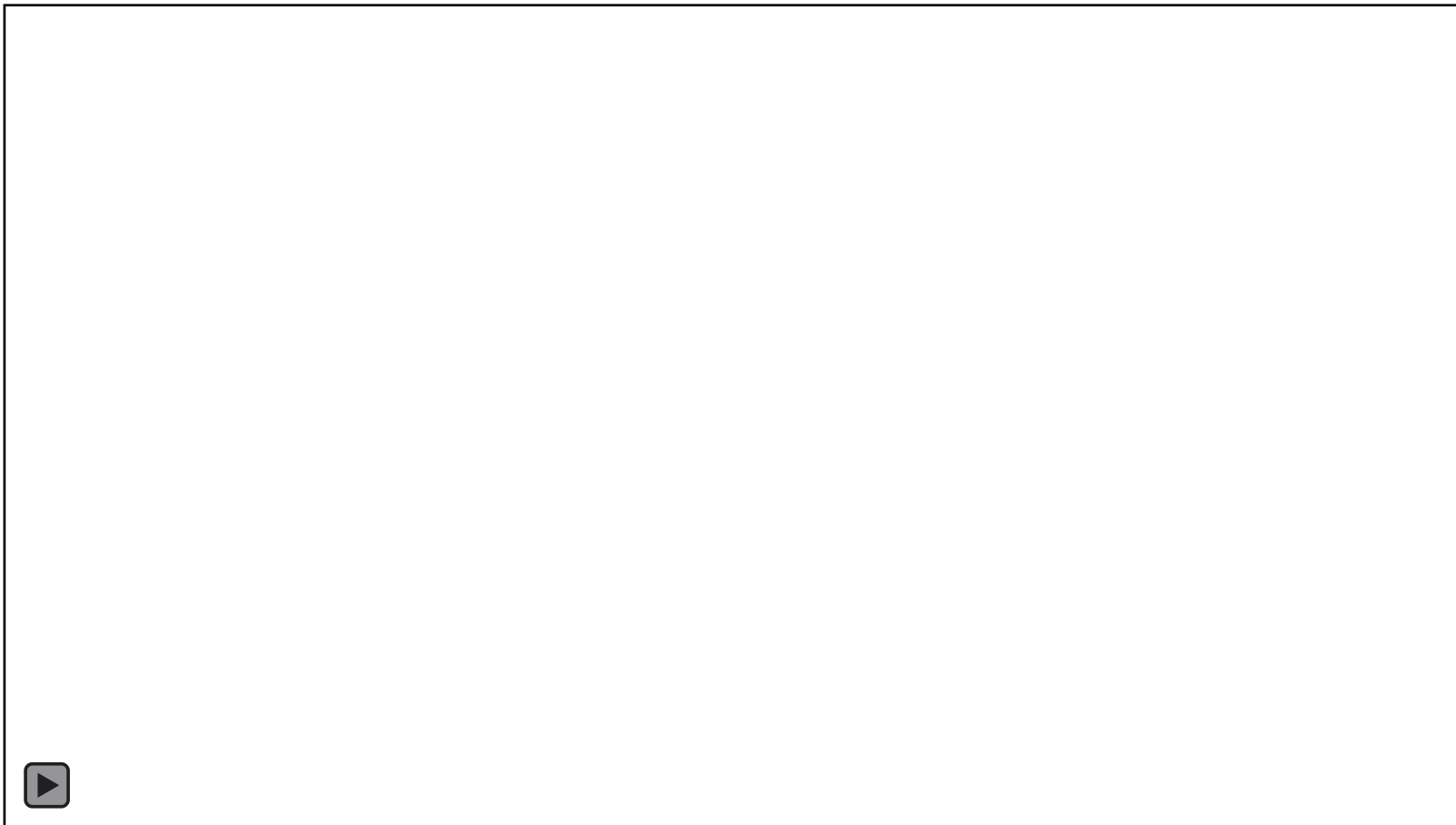


May 1 – 4, 2024

Wyndham Grand Rio Mar Puerto Rico Golf and Beach Resort
Rio Grande, Puerto Rico



The Future AI and Security





Ransomware Epilogue

MFA Implementation

Risk
Assessment/Implementation
Cyber Plan

What is your Liability under
your customer and vendor
contracts?

Security Cost of Continued
Use of Legacy Systems

Understand Your Insurance
Coverage and Panel Firms

No Incident Plan is Planning
to Fail

Key Takeaways

It won't happen to our organization is no excuse!

How many customers do you want to lose before security is a priority??

Ransomware is now a trillion-dollar industry for a reason!

Do you have a plan? Who are you going to call?? Hint: It's not Ghostbusters!

Have you exercised your plan (would you show up Super Bowl Sunday with no game plan)?