Managing port and maritime cyber risk

Andrew Baskin

20 September 2019

CIP Inter-American Committe on Ports

HudsonAnalytix

Contents

I. Introduction

II. Tears

III. Film

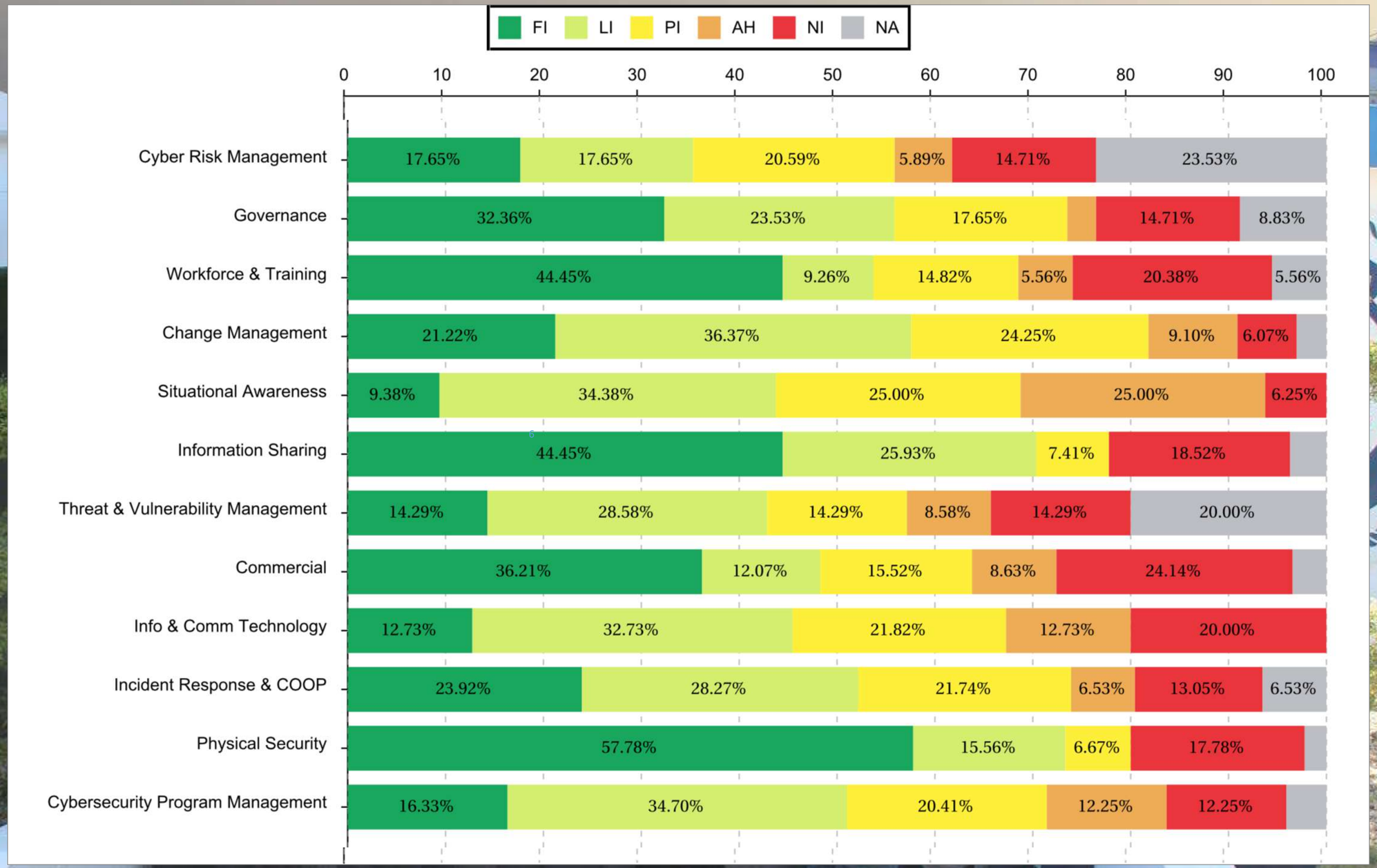
IV. Comfort

Global presence

HudsonCyber

Managing Cyber Risk

- ✓ Assessments
- ✓ Training
- ✓ Threat Intelligence


FI
LI
PI
AH
NI
NA
0
10
20
30
40
50
60
70
80
90
100
Cyber Risk Management
17.65%
17.65%
20.59%
5.89%
14.71%
23.53%
Governance
32.36%
23.53%
17.65%
14.71%
8.83%
Workforce & Training
44.45%
9.26%
14.82%
5.56%
20.38%
5.56%
Change Management
21.22%
36.37%
24.25%
9.10%
6.07%
Situational Awareness
9.38%
34.38%
25.00%
25.00%
6.25%
Information Sharing
44.45%
25.93%
7.41%
18.52%
Threat & Vulnerability Management
14.29%
28.58%
14.29%
8.58%
14.29%
20.00%
Commercial
36.21%
12.07%
15.52%
8.63%
24.14%
Info & Comm Technology
12.73%
32.73%
21.82%
12.73%
20.00%
Incident Response & COOP
23.92%
28.27%
21.74%
6.53%
13.05%
6.53%
Physical Security
57.78%
15.56%
6.67%
17.78%
Cybersecurity Program Management
16.33%
34.70%
20.41%
12.25%
12.25%

I. Introduction

II. Tears

III. Film

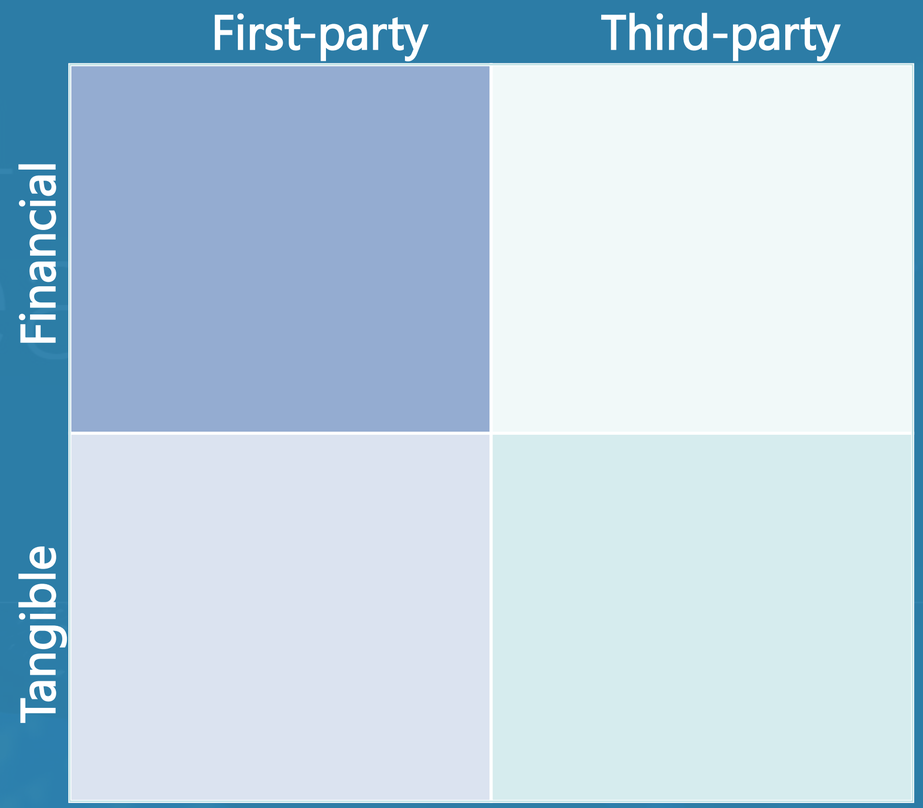
IV. Comfort

1. Common
2. Costly
3. Complex

1,946,181,599

The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018

Cyber loss spectrum



Revenue los and costs related to incident response, including public relations, data recovery, and legal costs

Physical damage:
- Property damage
- Bodily injury

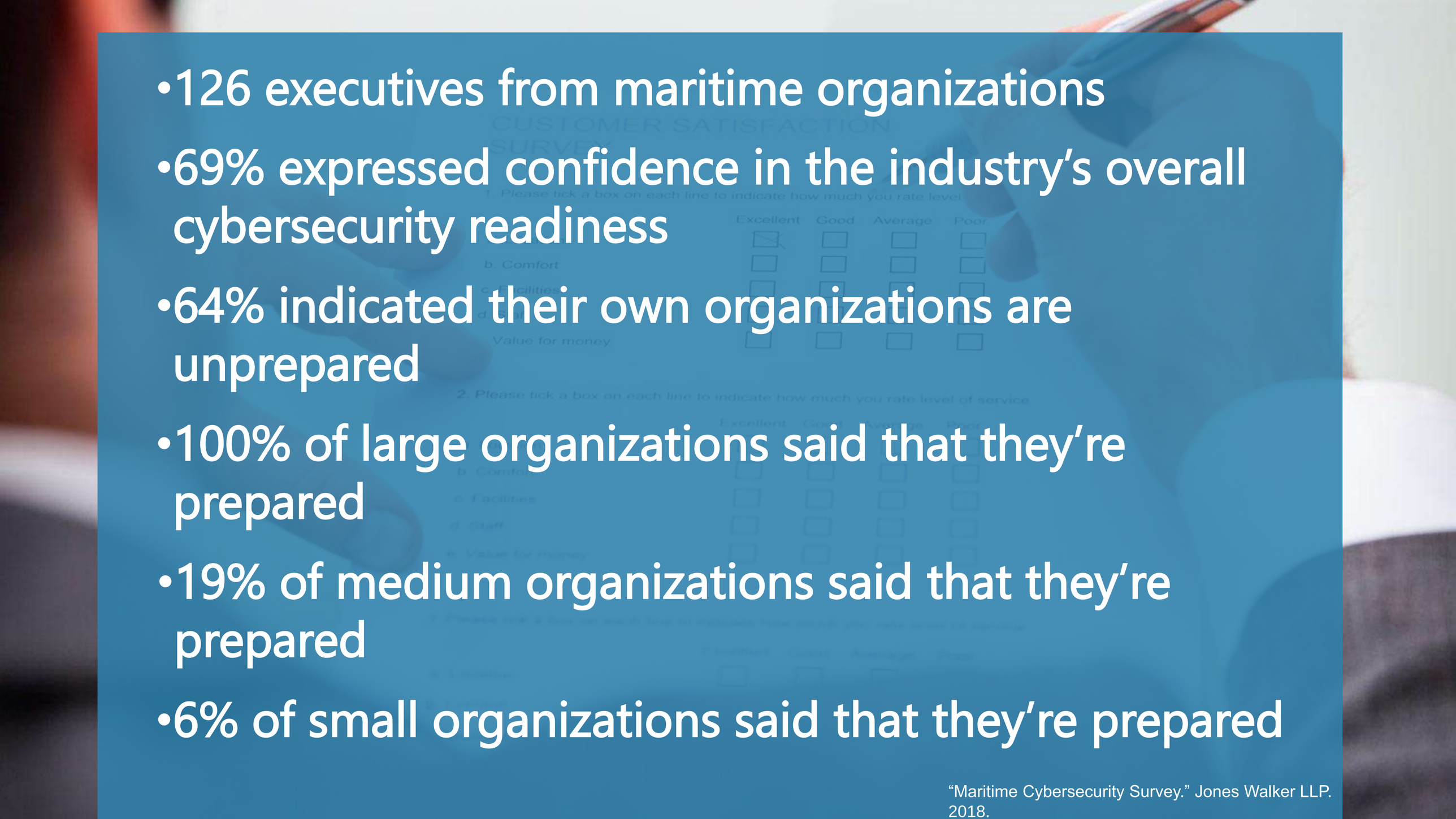
Third parties can try to recover:
- Civil penalties
- Revenue loss
- Recovery costs

Physical damage can affect third parties
- Property damage
- Bodily injury

1. Use multiple tactics concurrently

2. Attack supply chain partners to get to intended target

3. Increased focus on advanced persistent threats



- 126 executives from maritime organizations
- 69% expressed confidence in the industry's overall cybersecurity readiness
- 64% indicated their own organizations are unprepared
- 100% of large organizations said that they're prepared
- 19% of medium organizations said that they're prepared
- 6% of small organizations said that they're prepared

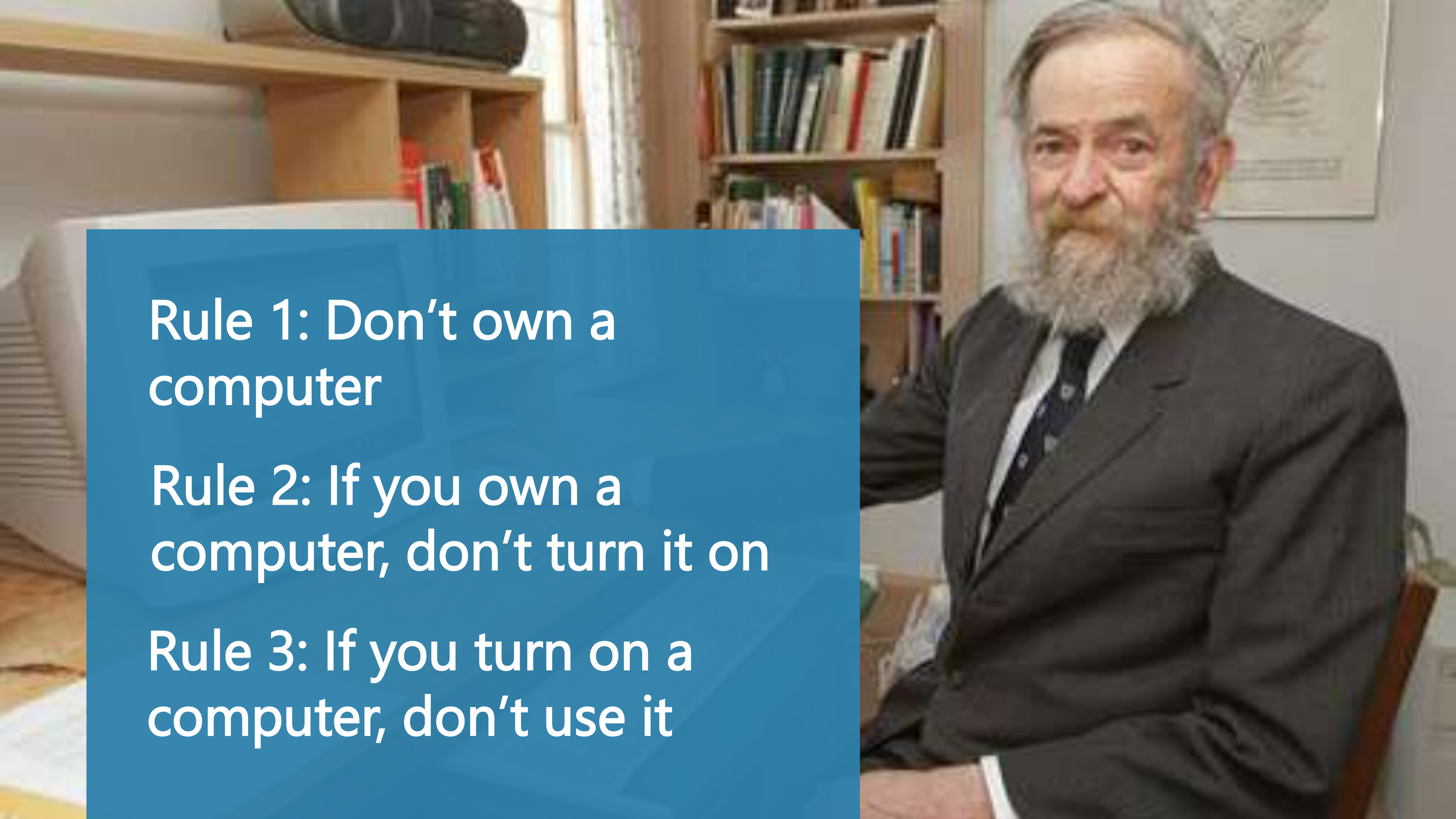
"Maritime Cybersecurity Survey." Jones Walker LLP. 2018.

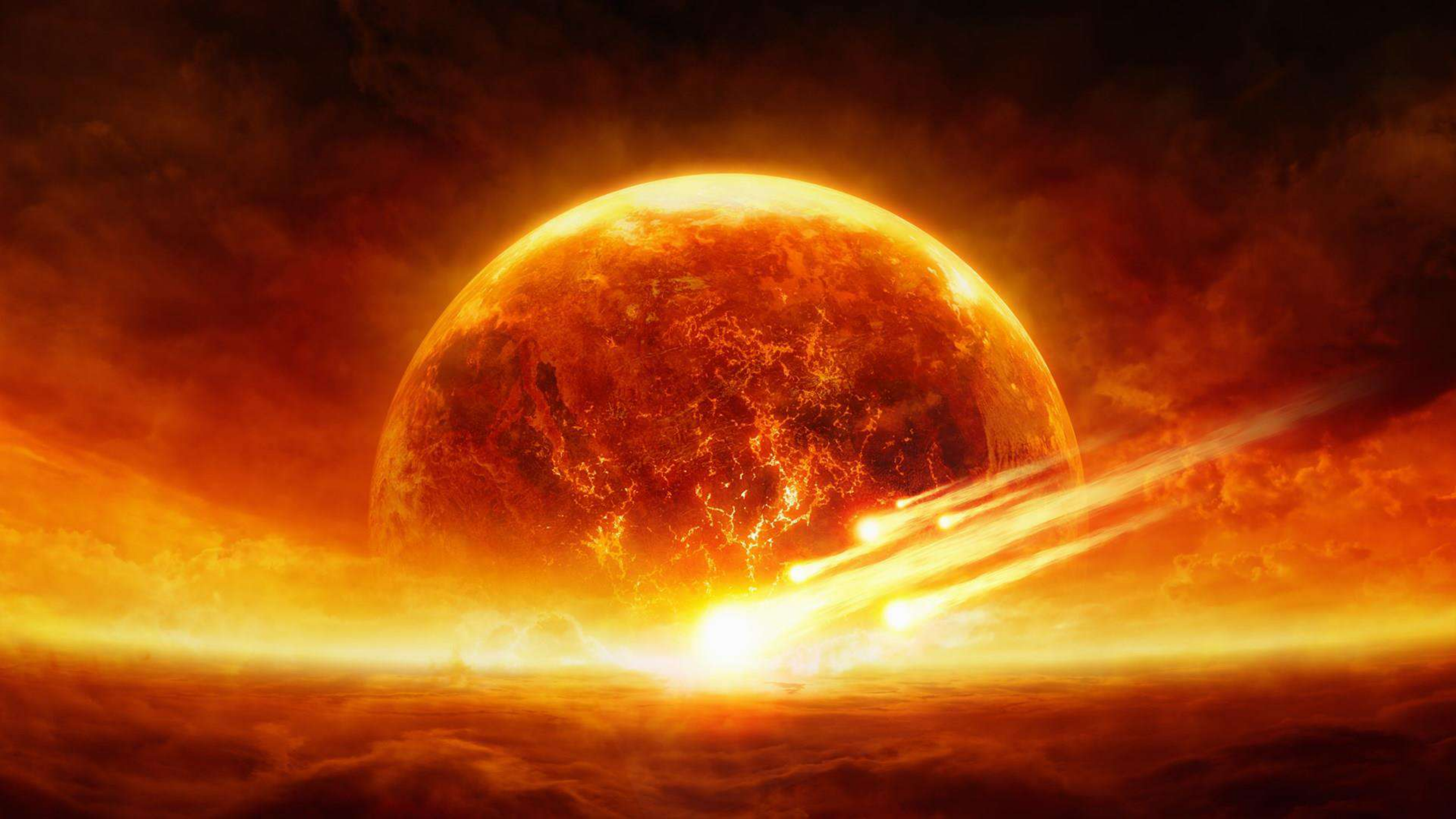
Port of Los Angeles

- Victim of the NotPetya attack
- APM terminal couldn’t operate for several days
- Had to carry out activities manually
- APM suffered roughly $300 million in losses

Port of San Diego

- Ransomware attack
- Couldn’t access various administrative systems
- Didn’t suffer any operational effects


Rule 1: Don’t own a computer
Rule 2: If you own a computer, don’t turn it on
Rule 3: If you turn on a computer, don’t use it

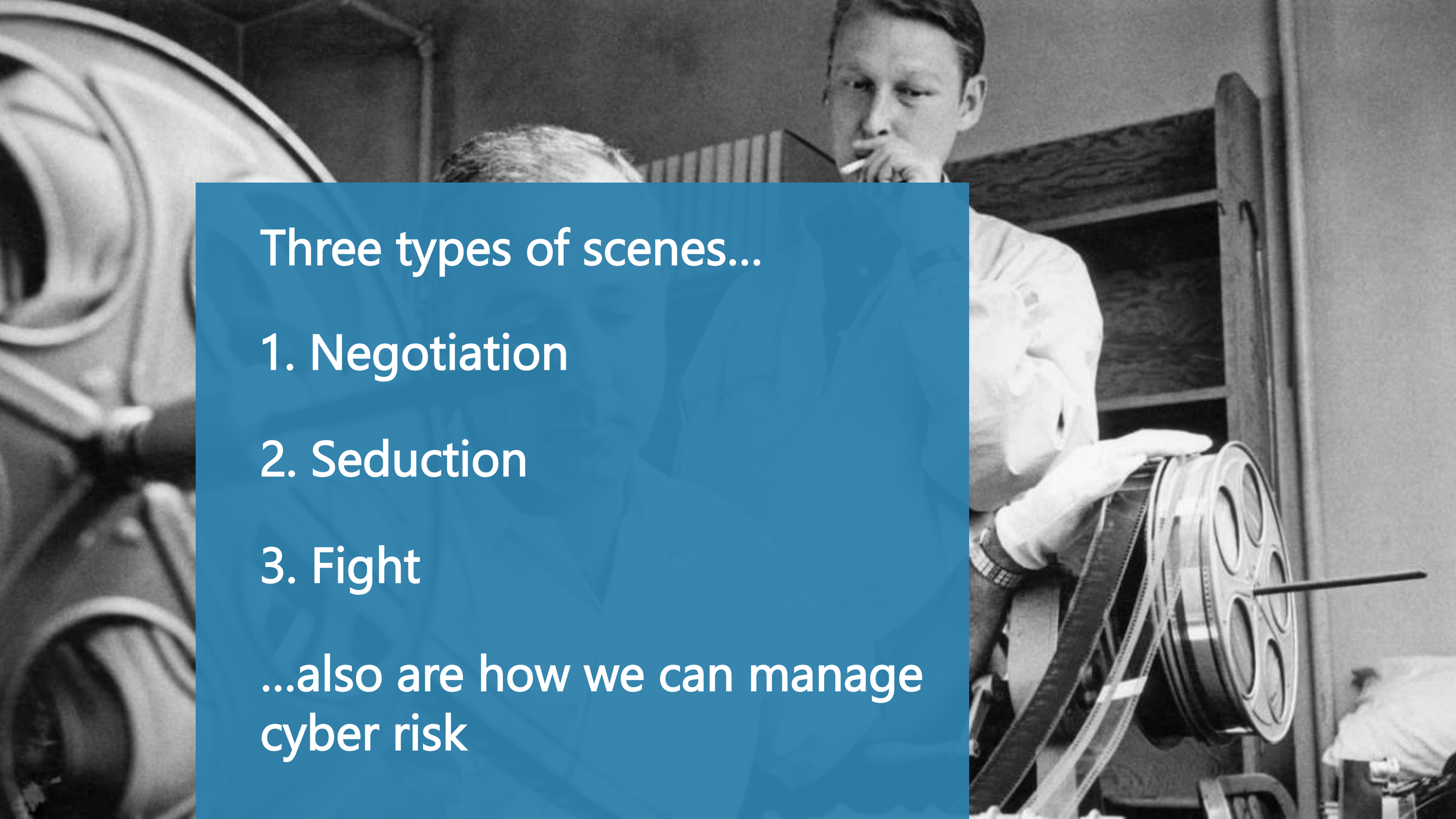


I. Introduction

II. Tears

III. Film

IV. Comfort



Three types of scenes…

1. Negotiation

2. Seduction

3. Fight

…also are how we can manage cyber risk

Negotiation: including cybersecurity in your agreements

1. Identify third parties
2. Prioritize third parties based on potential risk
3. Research new third parties
4. Review contracts often
5. Ensure that attorneys review contracts
6. Have contingency plans
7. Continuously review

SEDU AFF TO

Resources

$

5

FIGHT: HAVE A CYBER INCIDENT RESPONSE PLAN

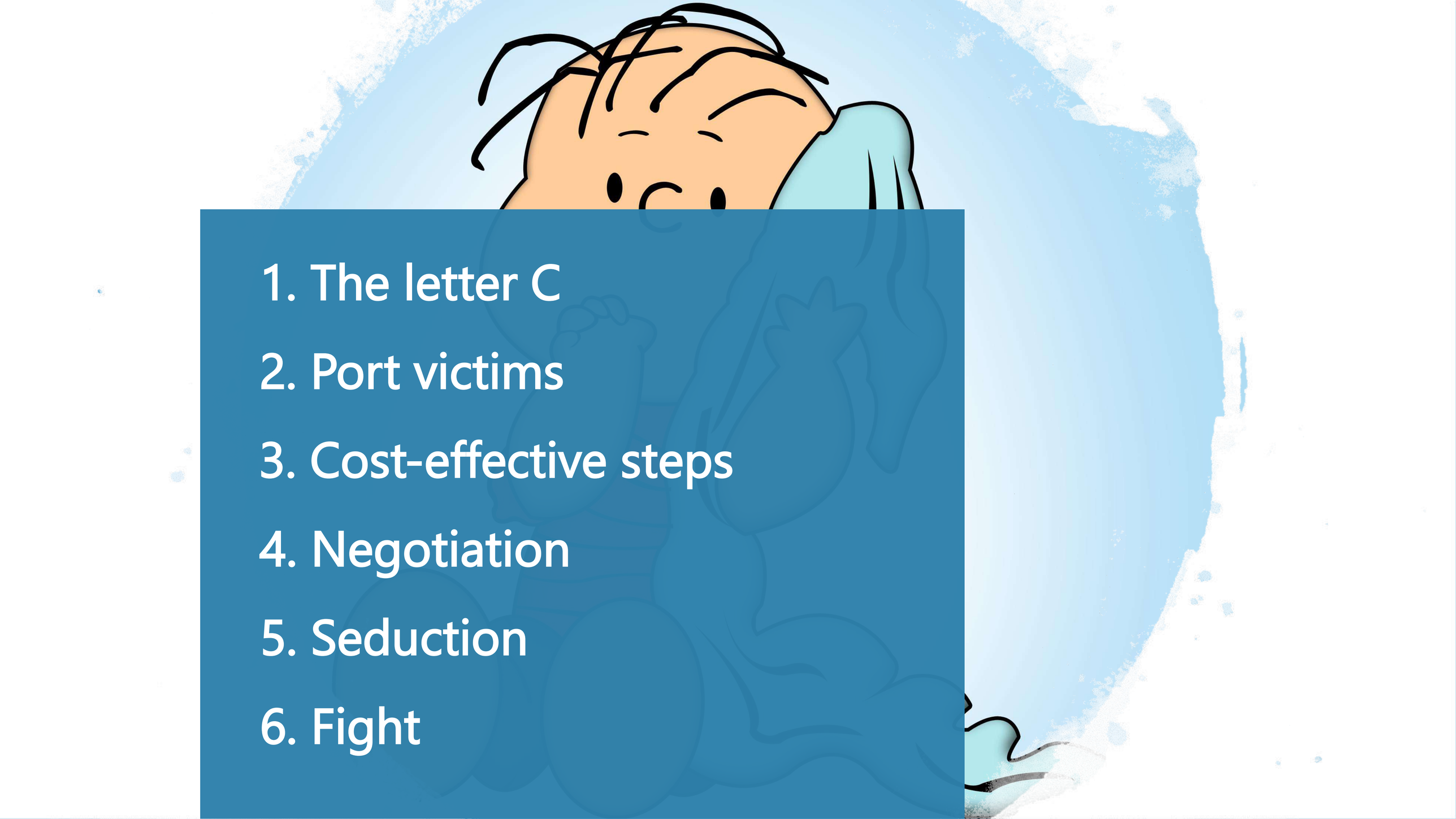
1. Documented and integrated
2. Responsibilities
3. External resources
4. Exercises

I. Introduction

II. Tears

III. Film

IV. Comfort



1. The letter C
2. Port victims
3. Cost-effective steps
4. Negotiation
5. Seduction
6. Fight

Andrew Baskin

andrew.baskin@hudsonanalytix.com

+1.703.581.8054

HudsonAnalytix