# 2025 Rochester Security Summit

## Lessons Learned from a CISO Who Managed to Keep His Job

Alan Levine
icecreamtruckman@aol.com

# Who I am

- Carnegie Mellon University faculty.
- Former CISO for two Fortune 500 companies.
- About a thousand years of experience
- Learned by the school of hard knocks.
- An original CISO in many ways.

# An early adopter of bad things

At a hospital:

- Dumpster diving.

At a medical center:

- Insider medical records breach.

At a Fortune 500:

- 3rd party benefits breach.
- I Love You, Slammer, Blaster.

Each incident was novel, damaging, teachable.

I learned, and I kept my job.  And then things got worse.

# The essential truth

- I ran good, strong programs.
- Still, the greatest of all incidents came.
- Life changed literally overnight.
- FBI and Mandiant would both name it *APT 1*.

*An advanced persistent threat is a threat actor**,** typically a state or state-sponsored group, that gains unauthorized access to a computer network and then remains undetected for an extended period.*

# An attack’s details

**What we learned**

- An email phish
- Initial malware
- More malware
- Privilege elevation
- Lateral movement
- Credential exfiltration
- Data exfiltration

**What we did**

- **A phone call**
- **Inquiries**
- **Investigation**
- Sneakernet
- Cooperation
- Indictment

# Brace when you answer the phone

- Akin to ‘Houston, *you* have a problem.’

- My CEO’s *what*?

- Don’t ask *that* question.

# Essential truths about execs

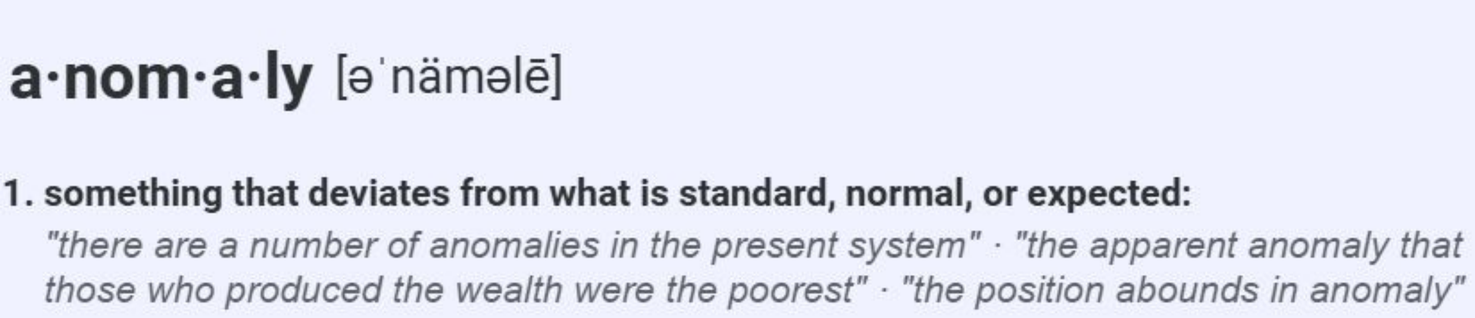
- Your CEO may write checks for cybersecurity, but cyber represents only a sliver of concern.

- Your CEO doesn’t look at email on vacation.

- Your CEO knows even less about your technology than you feared.

# 5 assets became 14

- A single element common among 5 was common among 9 more.
- Task manager processes shouldn’t have been ignored.
- One anomaly was in plain sight, but only if we looked.



**a·nom·a·ly** [əˈnäməlē]

**1. something that deviates from what is standard, normal, or expected:**
*"there are a number of anomalies in the present system" · "the apparent anomaly that those who produced the wealth were the poorest" · "the position abounds in anomaly"*

# An attack's details

**What we learned**

- **An email**
- Initial malware
- More malware
- Privilege elevation
- Lateral movement
- Credential exfiltration
- Data exfiltration

**What we did**

- A phone call
- Inquiries
- Investigation
- Sneakernet
- Cooperation
- Indictment

# More famous now

- No subject
- No body text
- No internal sender

# Essential truths about users

- Gullible.
- Greedy.
- Distracted.

‘Hell is other people.’
-- Sartre

All 14 received that same email.
Each reacted identically poorly.

# An attack’s details

**What we learned**

- An email phish
- **Initial malware**
- **More malware**
- **Privilege elevation**
- **Lateral movement**
- Credential exfiltration
- Data exfiltration

**What we did**

- A phone call
- Inquiries
- Investigation
- Sneakernet
- Cooperation
- Indictment

# ET phoned home

- Malware led to C2.
- C2 facilitated in and across sub-network movement.
- A directed quest.
- There was a particular objective.

# Essential truths about my environment

- I knew less about configs than I thought.
  - 20 credentials, cached everywhere.
  - Cross-breeding and nesting of privileged groups
  - Our network was less than a perfect 10, though we didn't know it.

# An attack’s details

**What we discovered**

- An email phish
- Initial malware
- More malware
- Privilege elevation
- Lateral movement
- Credential exfiltration
- Data exfiltration

**What we did**

- A phone call
- Inquiries
- **Investigation**
- **Sneakernet**
- Cooperation
- Indictment

# Intelligence updates

- A single page
- A single passenger
- Back and forth nearly every day for three months.

# An attack's details

**What we discovered**

- An email phish
- Initial malware
- More malware
- **Privilege elevation**
- **Lateral movement**
- **Credential exfiltration**
- Data exfiltration

**What we did**

- A phone call
- Inquiries
- **Investigation**
- Sneakernet
- Cooperation
- Indictment

# Watch your assets

- Just one BDC, misconfigured or unpatched or both, is all it took.

- Then our global directory was, as they say, out the door.

# Pass-the hash

- **Pass the hash (PtH)** is a type of cybersecurity attack in which an adversary steals a “hashed” user credential and uses it to create a new user session on the same network.
- Unlike other credential theft attacks, a pass the hash attack doesn’t require the attacker to know or crack the password to gain access to the system.

# An attack's details

**What we discovered**

- An email phish
- Initial malware
- More malware
- Privilege elevation
- Lateral movement
- Credential exfiltration
- **Data exfiltration**

**What we did**

- A phone call
- Inquiries
- Investigation
- Sneakernet
- Cooperation
- Indictment

# What the attacker sought

- A significant business deal.
- A matter of trust (or lack of it).
- Email might contain crown jewels.
- More than just our CEO’s jewels.

# An attack's details

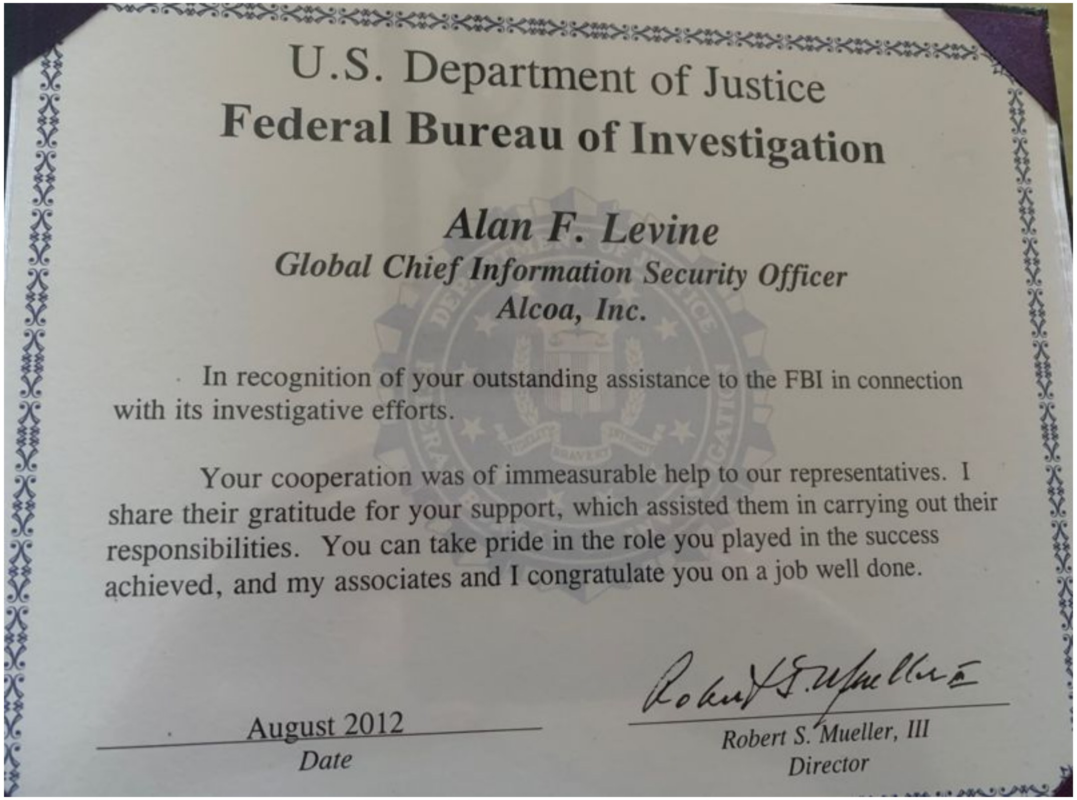
**What we discovered**

- An email phish
- Initial malware
- More malware
- Privilege elevation
- Lateral movement
- Credential exfiltration
- Data exfiltration

**What we did**

- A phone call
- Inquiries
- Investigation
- Sneakernet
- **Cooperation**
- **Indictment**

# More famous now



U.S. Department of Justice

**Federal Bureau of Investigation**

***Alan F. Levine***

***Global Chief Information Security Officer***

***Alcoa, Inc.***

In recognition of your outstanding assistance to the FBI in connection with its investigative efforts.

Your cooperation was of immeasurable help to our representatives. I share their gratitude for your support, which assisted them in carrying out their responsibilities. You can take pride in the role you played in the success achieved, and my associates and I congratulate you on a job well done.

August 2012

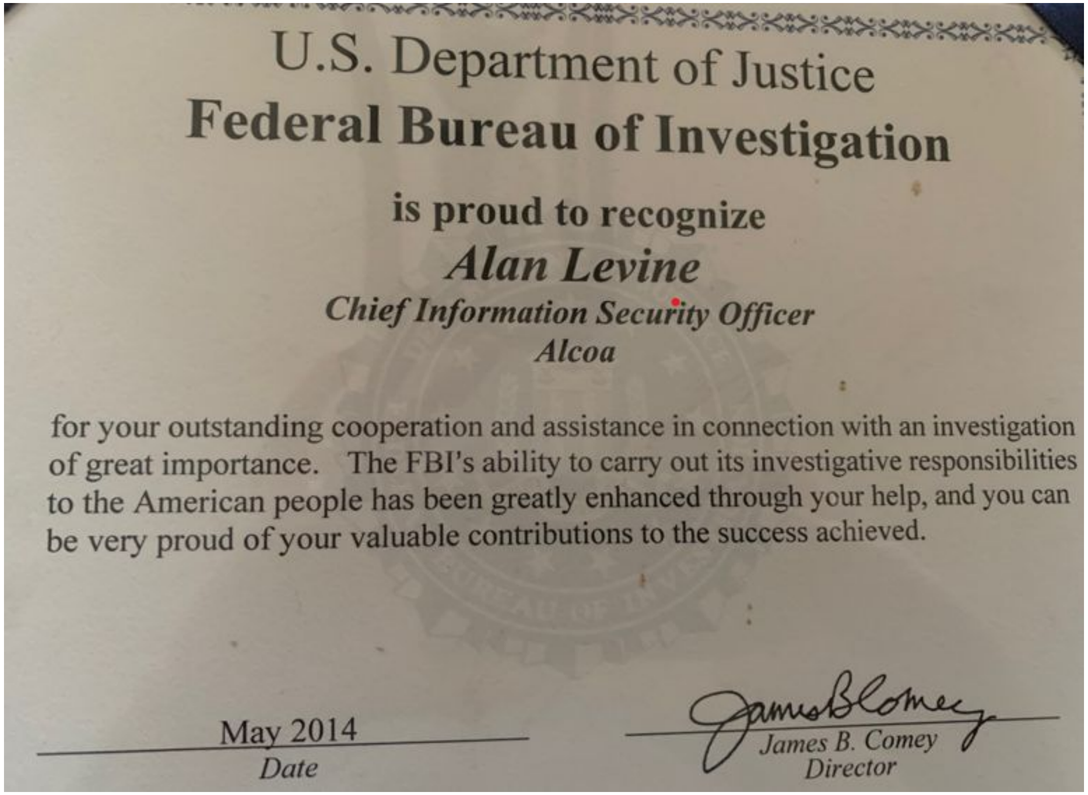
*Date*

Robert S. Mueller III

*Robert S. Mueller, III*

*Director*

# Even more famous now



U.S. Department of Justice

**Federal Bureau of Investigation**

**is proud to recognize**

***Alan Levine***

***Chief Information Security Officer***

***Alcoa***

for your outstanding cooperation and assistance in connection with an investigation of great importance. The FBI's ability to carry out its investigative responsibilities to the American people has been greatly enhanced through your help, and you can be very proud of your valuable contributions to the success achieved.

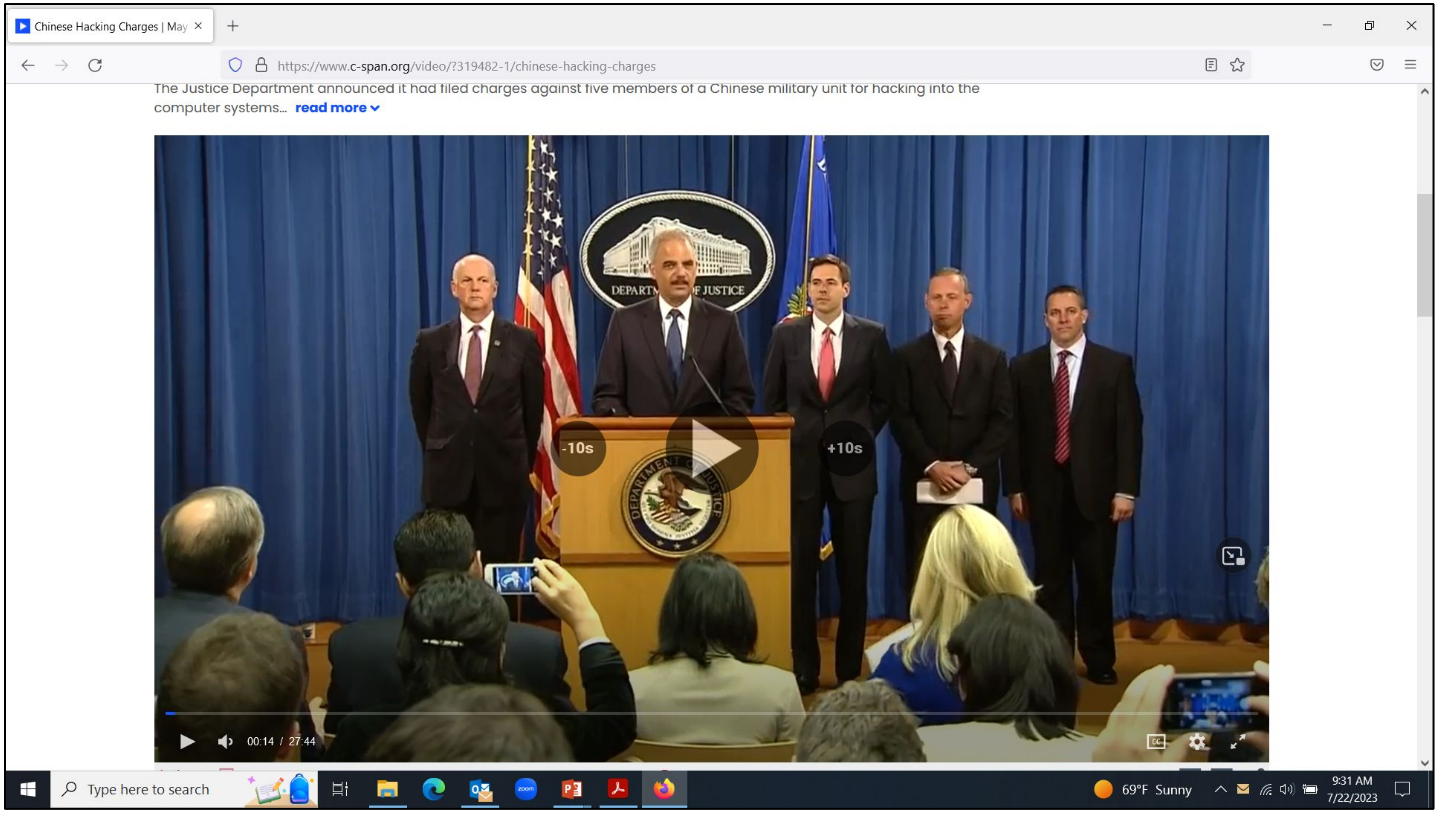
May 2014
*Date*

James B Comey
*James B. Comey*
*Director*

# Polishing your apple is not a good look

- I shared neither bureau commendation with my leadership.
- They expected excellence.
- I got not one high-five for getting things right, but I kept my job.

# A tipping point in cyber defense



The Justice Department announced it had filed charges against five members of a Chinese military unit for hacking into the computer systems... **read more**

Chinese Hacking Charges | May
https://www.c-span.org/video/?319482-1/chinese-hacking-charges
DEPARTMENT OF JUSTICE
-10s
+10s
00:14 / 27:44
Type here to search
69°F Sunny
9:31 AM
7/22/2023

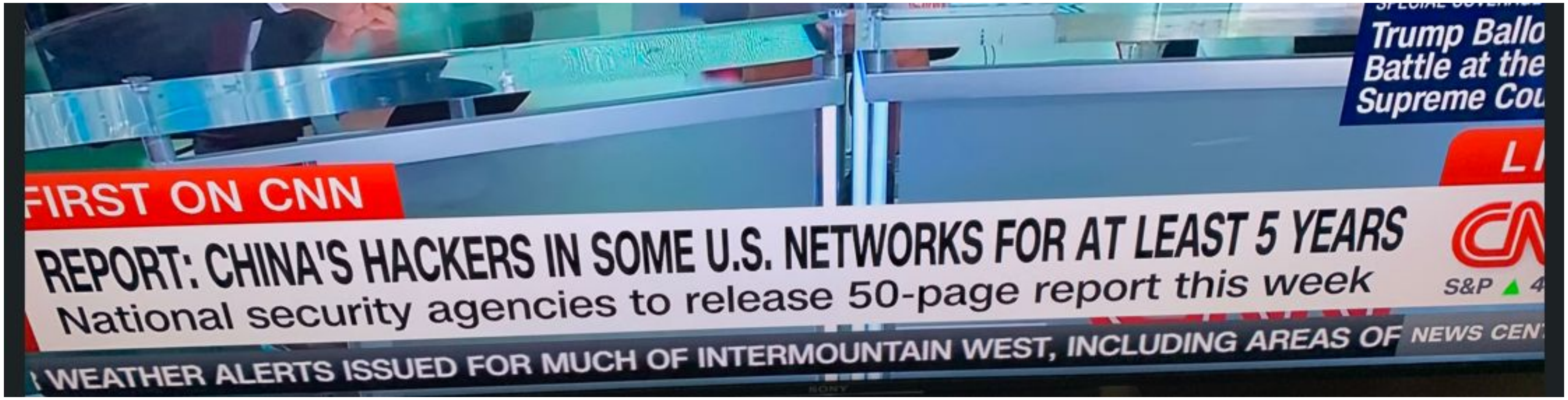
https://www.c-span.org/program/news-conference/chinese-hacking-charges/347426

# Not famous, but they should be

Named in the indictment. Photographed in uniform.

# Old news is new

- Dwell time is increasing, and risk is growing for all of us.



Trump Ballo
Battle at the
Supreme Cou

FIRST ON CNN

REPORT: CHINA'S HACKERS IN SOME U.S. NETWORKS FOR AT LEAST 5 YEARS

National security agencies to release 50-page report this week

WEATHER ALERTS ISSUED FOR MUCH OF INTERMOUNTAIN WEST, INCLUDING AREAS OF

# What I learned

- My program could never be good enough.
  - No matter how I adapted
  - Now matter how I improved
- I should have engaged formal connections with law enforcement better, sooner, for everyone's good.
  - Establish public/private relationships now, not when

# What else I learned

Every assessment, audit, review told me what I knew.

- The surprise, what I didn't know, was my vulnerability.

Finding innovative, resource-effective approaches is the ongoing cyber defense challenge.  We can never meet it.

Keep your job?  Do the job and keep your fingers crossed.  Mine were crossed all the time.

# History is our best teacher

- MOVEit is not so different from SolarWinds.
  - Vulns in third party software
- Ransomware is not so different from ILOVEYOU.
  - Each equally debilitating, capable of destroying data and orgs
- Cyber risk to IoT has its foundations in Windows 3.1 (yes, that's "for Workgroups").
  - Connectivity creates risk

# There's more we can do

- Demand secure software ('secure by default').
  - But will an SBOM really solve?
- Buy and/or build more and better defenses.
  - But will the marketplace respond?
- Demand better from our supply chains.
  - But business comes first, doesn't it?
- Demand vigilance.
  - But vigilance takes time, people, money, patience, all things we may not have.

# True or false?

We are staffed better.

We are trained better.

We are funded better.

An attacker needs to be right once.   We need to be right every time.

AI will impact us positively.

AI will impact us negatively.

‘Good enough’ isn’t good enough anymore.

# If you see these guys (you won’t), say something

They probably didn’t keep their livelihoods.

They may not have kept their lives.

We can hope.

Questi