Resiliency During Crisis

Josh Peltz
VP of the West, Zero Networks

DOCENT | studios
PRESENTS
CornCon 11
Manifest your inner Cyber Superhero

Comparing 'Flight 1549' with a Cybersecurity Breach

The "Miracle on the Hudson" shares surprising parallels with a cybersecurity breach.

Both involve high-stakes crises…

Requiring preparation,

Rapid response,

and thorough investigation.

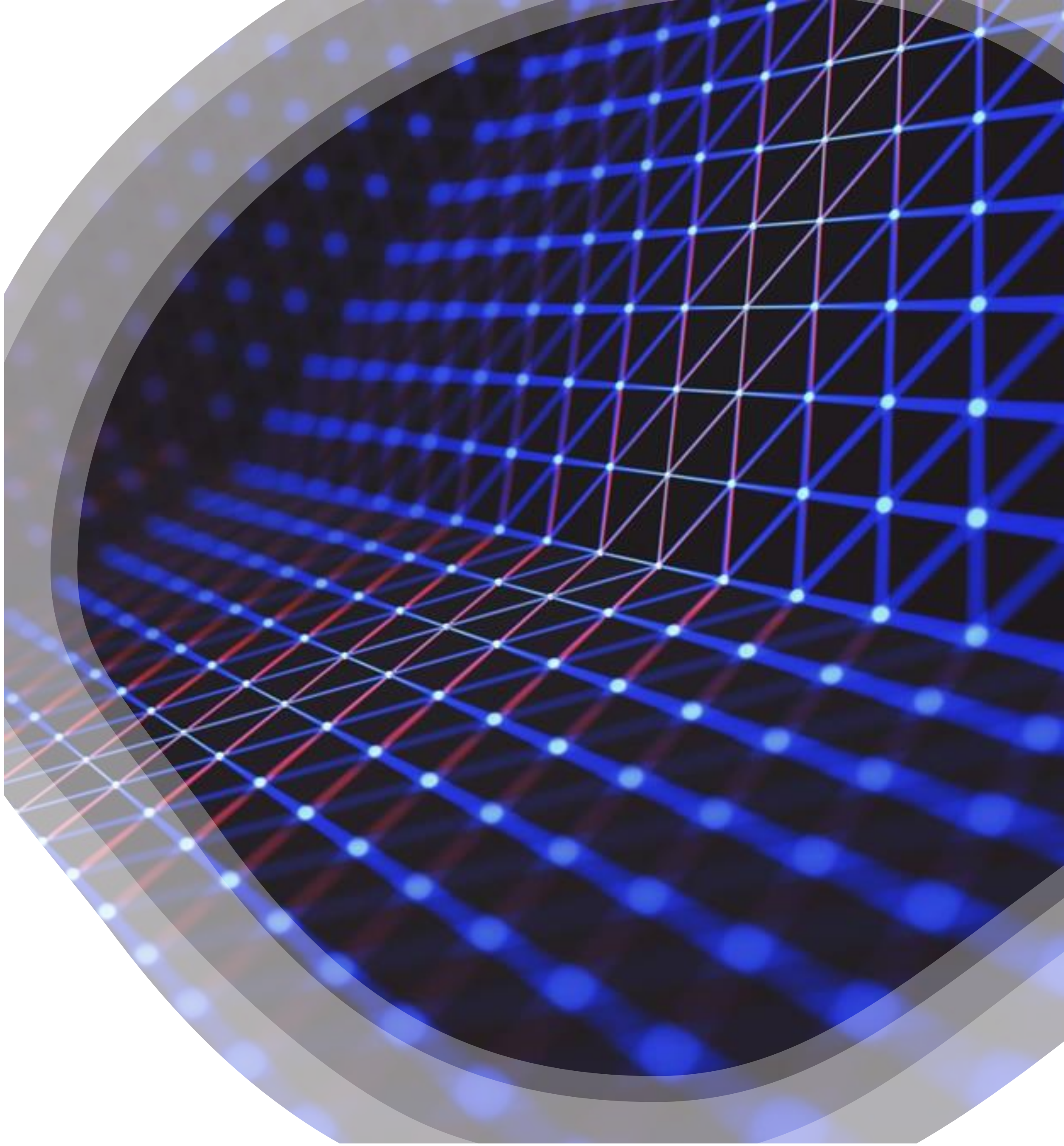
Today, I'll outline **similarities** between the two events, focusing on:

preparation and training,

incident detection and response,

business continuity and disaster recovery,

and **aftermath investigations**.



But first, a preface:

Lightning Strikes

In 1992, I was visiting Boca Raton, FL where I was hit by a bolt of lightning.

I was told by the doctors that I was “the first to survive that year”.

Fast Forward: January 15th, 2009

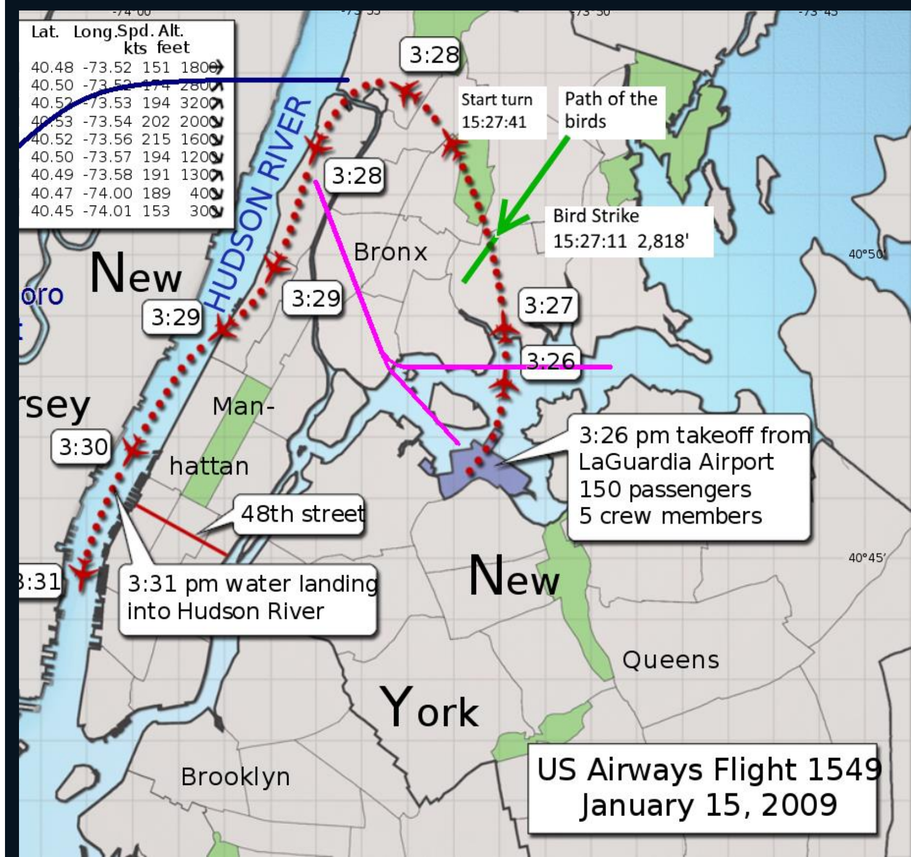
‘Fun Facts’ from Flight 1549

- We struck a flock of Canada geese at an altitude of **2,800 ft**
- The aircraft slowed but continued to climb for a further 19 seconds, reaching about **3,100 ft** at an airspeed of about 213 mph (185 knots)
- We began a glide descent, accelerating to 240 mph (210 knots)
- The aircraft passed less than **600 feet** above the George Washington Bridge
- We hit the water at **177 mph**
- Total Flight Time: **5 minutes**

- Air temp was **19 °F** and water temp was **41 °F**
- Passengers and crew sustained **95** minor and five serious injuries
- **78** people received medical treatment, mostly for minor injuries and hypothermia
- **24** passengers and two rescuers were treated at hospitals
- with **Zero Fatalities**

…hence the media’s name,

“The Miracle on the Hudson”



Lat.	Long.	Spd. kts	Alt. feet
40.48	-73.52	151	1800 →
40.50	-73.52	174	2800 ↗
40.52	-73.53	194	3200 ↗
40.53	-73.54	202	2000 ↘
40.52	-73.56	215	1600 ↘
40.50	-73.57	194	1200 ↘
40.49	-73.58	191	1300 ↗
40.47	-74.00	189	400 ↘
40.45	-74.01	153	300 ↘

Start turn 15:27:41

Path of the birds

Bird Strike 15:27:11 2,818'

3:26 pm takeoff from LaGuardia Airport
150 passengers
5 crew members

3:31 pm water landing into Hudson River

US Airways Flight 1549
January 15, 2009

Why Is My Story Relevant to Yours...?

- Preparation and Training
- Incident Detection
    - Rapid Decision-Making
    - Communication and Collaboration
    - Use of Available Resources
    - Minimizing Impact: Containment and Eradication
- Disaster Recovery
- Business Continuity
- Aftermath Investigations
    - Public and Stakeholder Communication
    - Pay It Forward
    - Lessons Learned

1. Preparation and Training

Flight 1549:

The crew, Air Traffic Control and the first responders all played vital roles, using their training to assist with emergency protocols.

Advanced preparation saves lives.

Cybersecurity Breach:

Organizations prepare for breaches through awareness training for employees and **IR drills**: pentests, security validations, tabletops.

Simulations and training ensure readiness for real-world crises.

Key Activities:

Develop and implement an IR plan - and then **be prepared to change the plan**.

Conduct tabletops to simulate attacks, protect systems and secure sensitive data.

Deploy monitoring tools and establish communication protocols.

Focus on **I&W** (indications and warnings).

Don't forget viewing the scenarios through a **non-cyber** lens; ensure that all personnel are aware of their roles in the event of an incident.

> *"For 42 years, I've been making small, regular deposits in this bank of experience, education and training.*
>
> *And on January 15, the balance was sufficient so that I could make a very large withdrawal."*
>
> – Captain Sully, AARP Magazine interview

2. Incident Detection

Flight 1549:

The bird strike and dual engine failure was identified **in seconds**.

Sully and Skiles noticed a sharp loss of thrust and unusual engine sounds, diagnosing the situation immediately.

Fast detection allows for faster action.

Cybersecurity Breach:

Intrusion detection systems and SIEMs alert teams to anomalies, such as unauthorized access or suspicious data transfers, unusual network activity or system failures.

Early detection tools are critical to limiting damage.

Key Activities:

Monitor for signs of a security breach or anomaly.

Analyze alerts from SIEM systems – but also context from new analytics, NAV, UEBA, automated tools and playbooks.

Gather relevant data to confirm the occurrence of an incident.

Classify the incident type to assess its potential impact.

3. Rapid Decision-Making

Flight 1549:

Sully had only moments to decide. He assessed options: return to LGA or divert to Teterboro.

Neither was viable.

Sully chose an emergency water landing in the Hudson—

A decision that saved all 155 lives on board.

Decisive action under pressure is vital.

Cybersecurity Breach:

IR teams must act quickly to contain a breach and threats.

Follow the **80/20 rule**, if there’s an 80% indication of catastrophic failure, don’t need to wait for 100%.

For example:

If ransomware is detected encrypting files, teams may decide to isolate affected systems, block malicious IPs, or even shut down networks to limit the attack.

Inaction can turn a small breach into a major crisis.

Communication and Collaboration

Flight 1549:

Sully and Skiles maintained clear communication with ATC about the emergency and their decision to land in the Hudson, ensuring coordinated efforts.

The crew also gave passengers clear instructions to **Brace for Impact**, reducing panic.

Effective communication ensures coordination and calm.

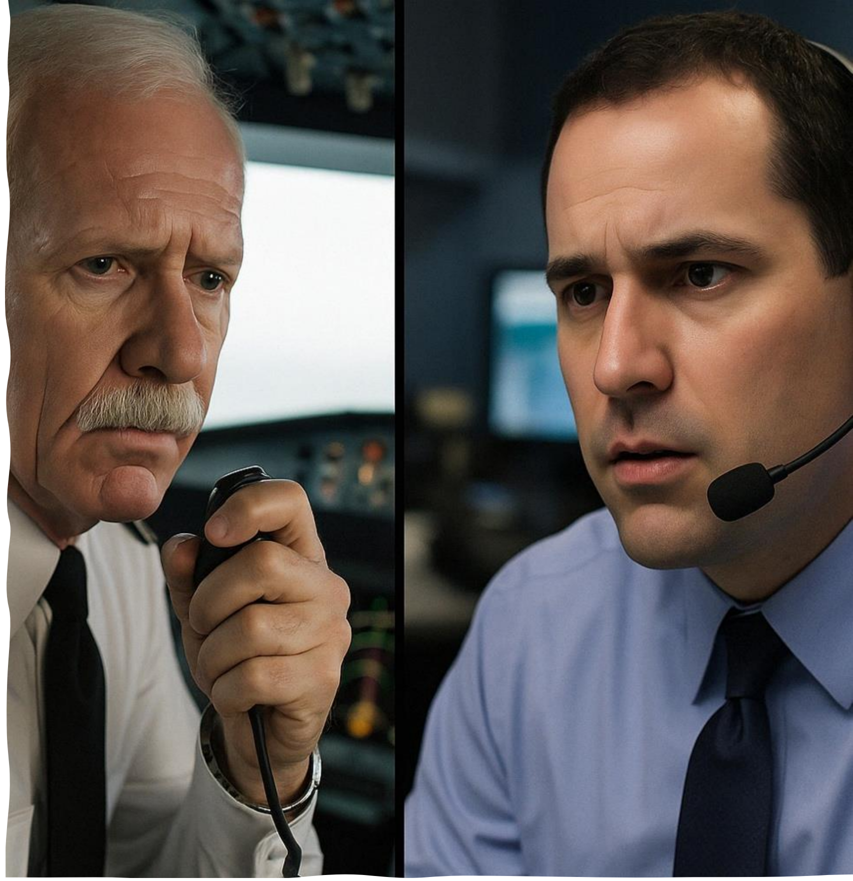
Cybersecurity Breach:

Answer this question: who is *actually in charge* when bad things happen?

IR Teams must notify IT staff, Security, Operations, Executives, Legal and PR, while also updating regulators, customers and other stakeholders.

Ensure you have an out-of-band communication method and technology.

Information-sharing is key to controlling chaos.



Use of Available Resources

Flight 1549:

We had lost all engine power. Sully relied on the plane's gliding capabilities and on the Hudson River as an improvised runway.

Emergency equipment, like life vests and rafts, ensured passenger safety during the evac.

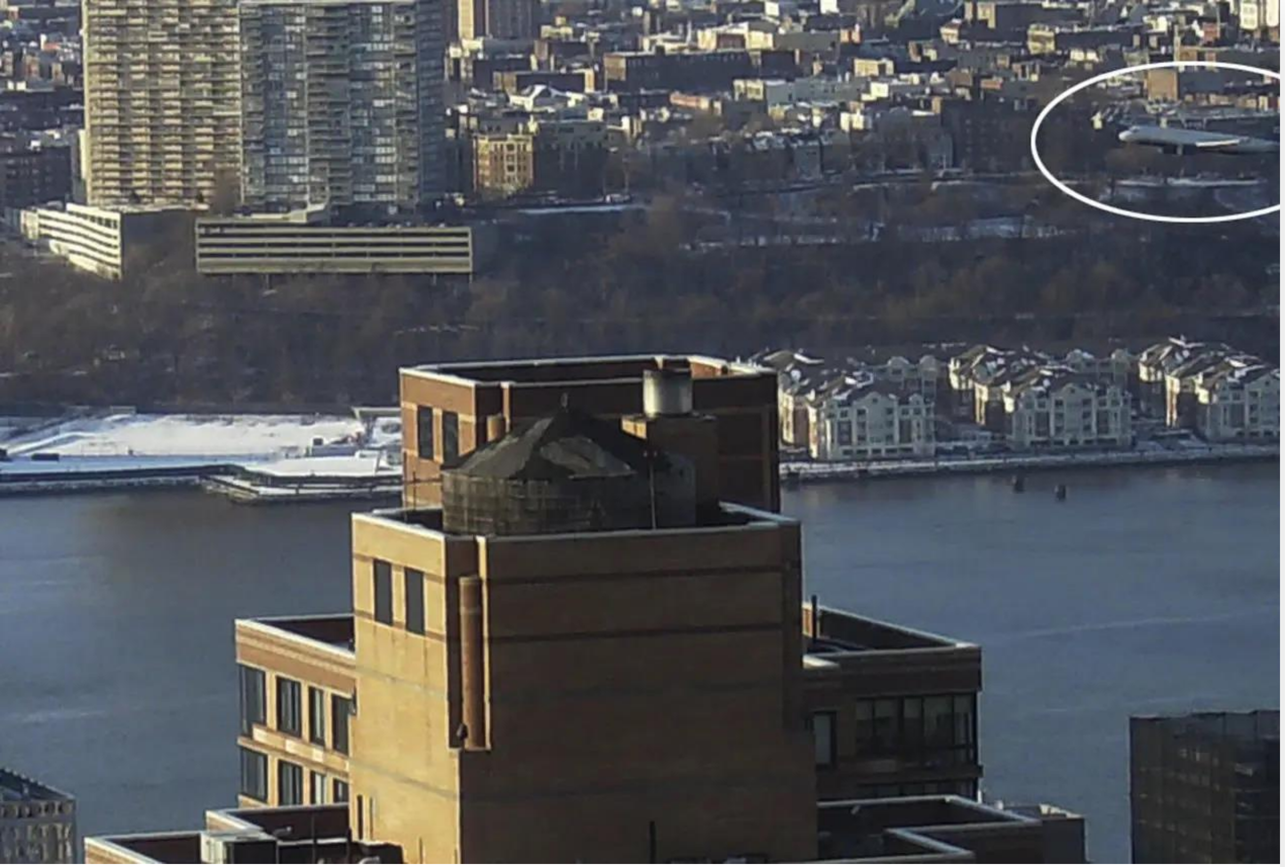
Creative use of resources can turn disaster into survival.

Cybersecurity Breach:

Two is one, and one is none. Have IR retainers as well as backups, cloud storage, and redundant systems ready to sustain operations.

- Note on IR Retainers: **Threat actors do not wait for contracts.** Pre-negotiated terms = faster response, clearer roles, and less chaos. The worst time to find a partner is during a crisis.

Prepared resources are lifelines during crises.



Minimizing Impact: Containment and Eradication

Just one decision made faster (or already predetermined) WILL reduce the blast radius.

Flight 1549:

Sully's actions ensured that all 155 passengers and crew survived.

He landed in the Hudson to minimize additional casualties, and even after the emergency landing, he and the crew worked to maintain calm and guide us to safety.

Cybersecurity Breach:

Fast, strategic response minimizes data loss, protects sensitive systems, and maintains public trust.

Damage control is a hallmark of good crisis management.

Think: ***Trees versus Forests.*** Speed of response is CRITICAL – the faster the threat actor is contained, the smaller the blast radius.

Key Activities:

Attribution comes later. Don't hunt while you're fixing the problem.

Identify / eliminate malware, unauthorized access points, or vulns.

Develop and test runbooks for disconnecting your network(s) and disabling authentication – including on-prem, Cloud, and SaaS workloads.

Ensure security controls remain online – include runbook exceptions for EDR, logging, identity, etc.

Proactively or reactively implement modern **Microsegmentation**.

Also, **policy engines are a beautiful thing.** Fix things at scale.

Disaster Recovery

Most organizations create backups, very few test recovery for mission critical workloads. Finding your single-point-of-failure(s) during recovery efforts is not where you want to be.

Flight 1549:

First responders ensured all passengers were evacuated safely and provided emergency services.

The plane was later salvaged from the river for investigation.

Fast recovery minimizes harm.

Cybersecurity Breach:

DR includes restoring systems, recovering data, and resuming normal operations.

Many organization lose hours and sometimes days switching priorities mid- stream during recovery operations due to lack of knowledge / pre-defined priorities to the business.

Recovery plans prevent long downtime.

Key Activities:

Restore systems from clean backups and validate their integrity.

Monitor systems closely for any signs of residual threats.

Threat actors target backups – if they can be encrypted, deleted, or modified, then they are not backups.

Gradually bring prioritized and eventually all systems back online to ensure stability and security.

OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
D.Fletcher for CloudTweaks.com

Business Continuity

Flight 1549:

Despite the emergency, US Airways continued operations, turning the incident into a positive case study on crisis management.

The airline reassured customers of their safety commitment.

Resilience builds trust.

Cybersecurity Breach:

BCPs ensure critical operations continue, even during a breach.

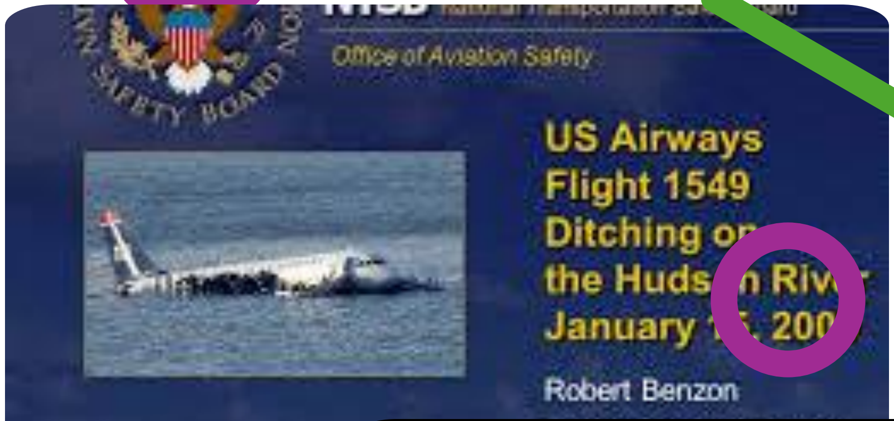
Ensure that critical services remain operational during containment efforts and maintain essential business functions during the recovery process.

Cyber insurance is the fallback plan that you DON'T want to rely on.

Use contingency plans, such as alternative systems or processes, to ensure minimal disruption to customers and operations.

Hospitals, for instance, may switch to manual processes during a ransomware attack to maintain patient care.

Continuity planning ensures survival.


NTSB National Transportation Safety Board

Office of Aviation Safety

US Airways
Flight 1549
Ditching on
the Huds n Riv
January 1 , 200

Robert Benzon

Aftermath Investigations

Flight 1549:

NTSB conducted a thorough investigation to determine cause.

They recommended safety improvements like enhanced engine designs, safety protocols and training programs based on lessons learned (including for dual-engine failures).

Post-crisis analysis drives improvement.

Cybersecurity Breach:

Post-breach investigations analyze how the breach occurred, identify vulnerabilities and attack methods, and recommend measures to prevent future incidents.

Learning from failure strengthens defenses.

Key Activities:

Conduct a post-incident analysis to evaluate the response's effectiveness.

Document findings: what worked well and what could be improved.

Update IR plans and training based on lessons learned.

And Finally - Pay It Forward

”For 42 years, I've been making small, regular deposits in this bank of experience, education and training.

And on January 15, the balance was sufficient so that I could make a very large withdrawal.”

– Captain Sully, AARP Magazine interview

Flight 1549:

The incident received extensive media coverage, and US Airways leveraged the positive outcome to reinforce its safety-first reputation.

Sully’s heroism was celebrated worldwide.

Cybersecurity Breach:

Companies must inform Customers, regulators, and stakeholders about breaches.

Post-breach, Security leaders can offer firsthand accounts to enlighten and support the community.

Honesty and transparency are vital.

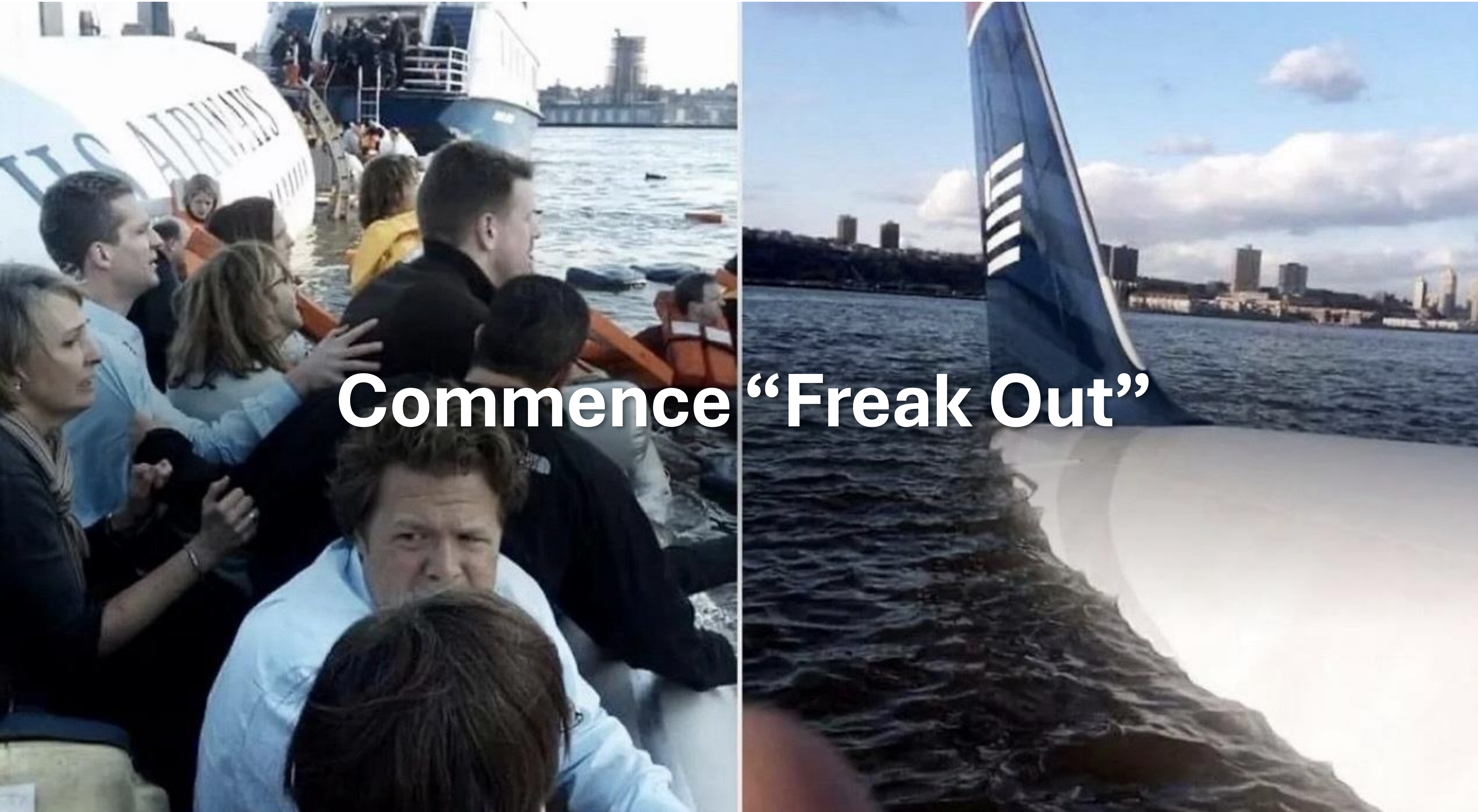
Every crisis is a lesson.

Key Activities:

Share insights with relevant stakeholders, customers and peers to enhance overall posture of the industry.

>> Yeah, I will never forget that day in February.
And any of you that have been through an event probably know exactly where

Instruction Manual for Your Next Disaster



Commence “Freak Out”

But Then, Quickly Bounce Back

Recognize that your actions, mindset, and choices play a crucial role in shaping outcomes.

In times of distress, springing into action, staying focused, and helping others can lead to survival and ultimately growth.

Breathe.

Take things

One

Step

At

a

Time.

Emphasize personal agency.

Take control of your narrative and create opportunities for positive results, regardless of circumstances.

Remember the Zen Farmer

There is No Such Thing as Good Luck or Bad Luck.

Instead, it's about how you perceive and respond to life's circumstances.

Farmer's horse runs away.

Neighbors say: "Such bad luck!"

Farmer replies: "Maybe."

Horse returns with 10 wild horses.

Neighbors: "Such good luck!"

Farmer: "Maybe."

Son breaks his leg taming a wild horse.

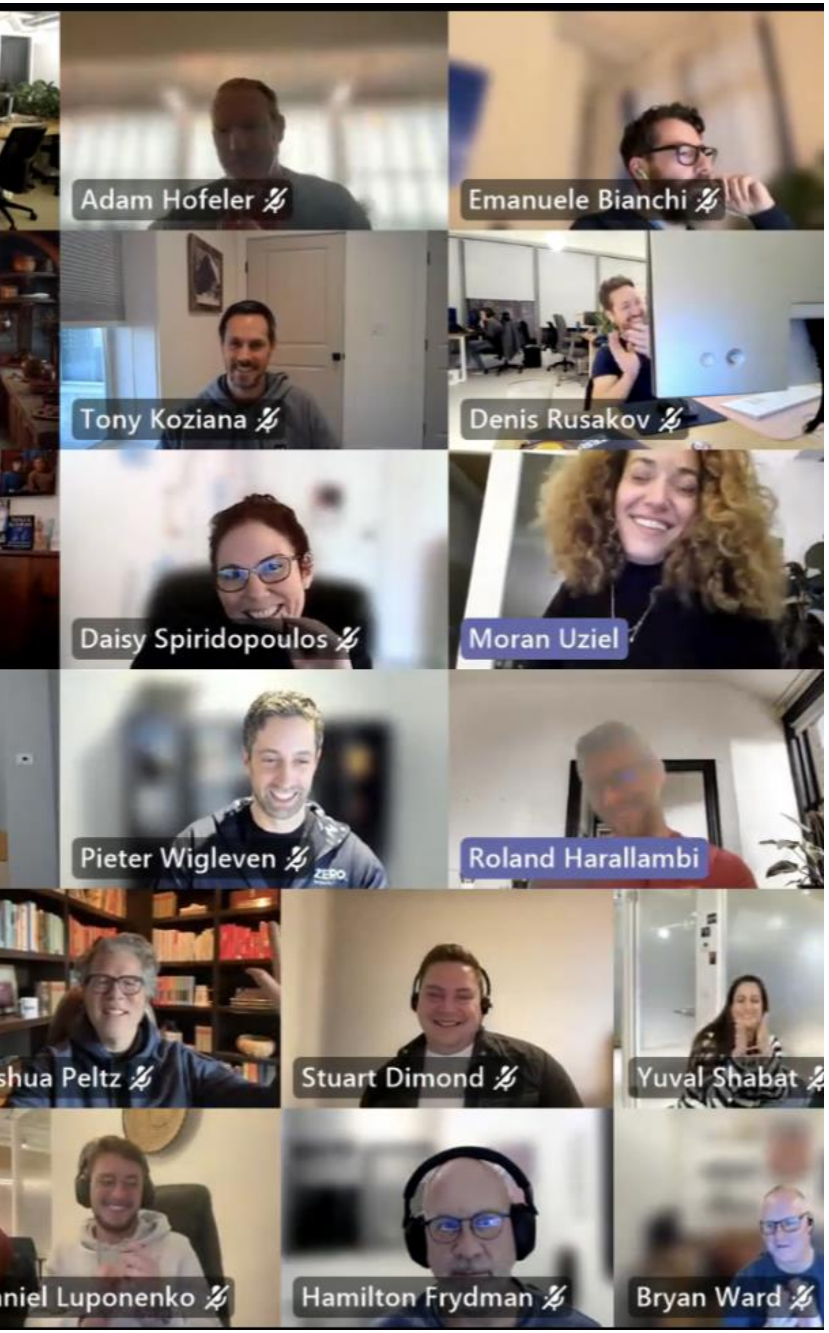
Neighbors: "Such bad luck!"

Farmer: "Maybe."

Army comes to draft young men, skips injured son.

Neighbors: "Such good luck!"

Farmer: "Maybe."



Recognize the Support of Community

Building and nurturing relationships can help you rise from personal and professional lows and find new highs.

Collective strength leads to positive outcomes that benefit everyone involved.

(Huge thanks to **Jason Norred**, **Dr. Chase Cunningham**, and **Rock Lambros** for your friendship and help)

Value Gradual Change

Significant life events may not always lead to immediate, drastic changes.

Focus on your gradual shifts in perspective and appreciation for life that occur over time.

Small, consistent moments of gratitude lead to profound transformation.

And, If You Ever Get the Chance...

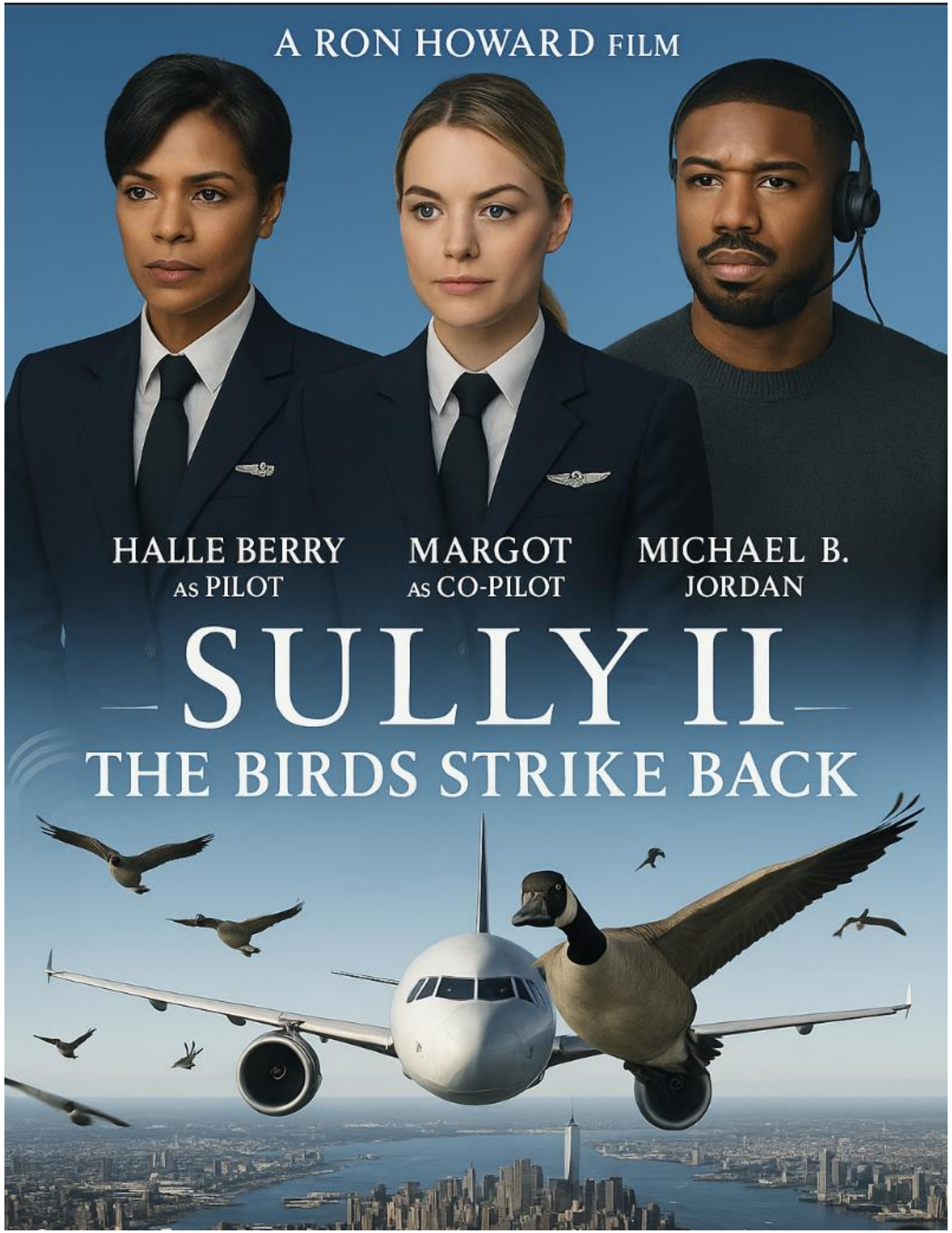
Get Interviewed on National TV

(Try Not to Cry)

When Clint Eastwood and Tom Hanks Invite You to Be in their Movie…

Say Yes

Become a Living Museum Exhibit



Star in a Sequel

And…

If John Johnson and Other Awesome Folks…

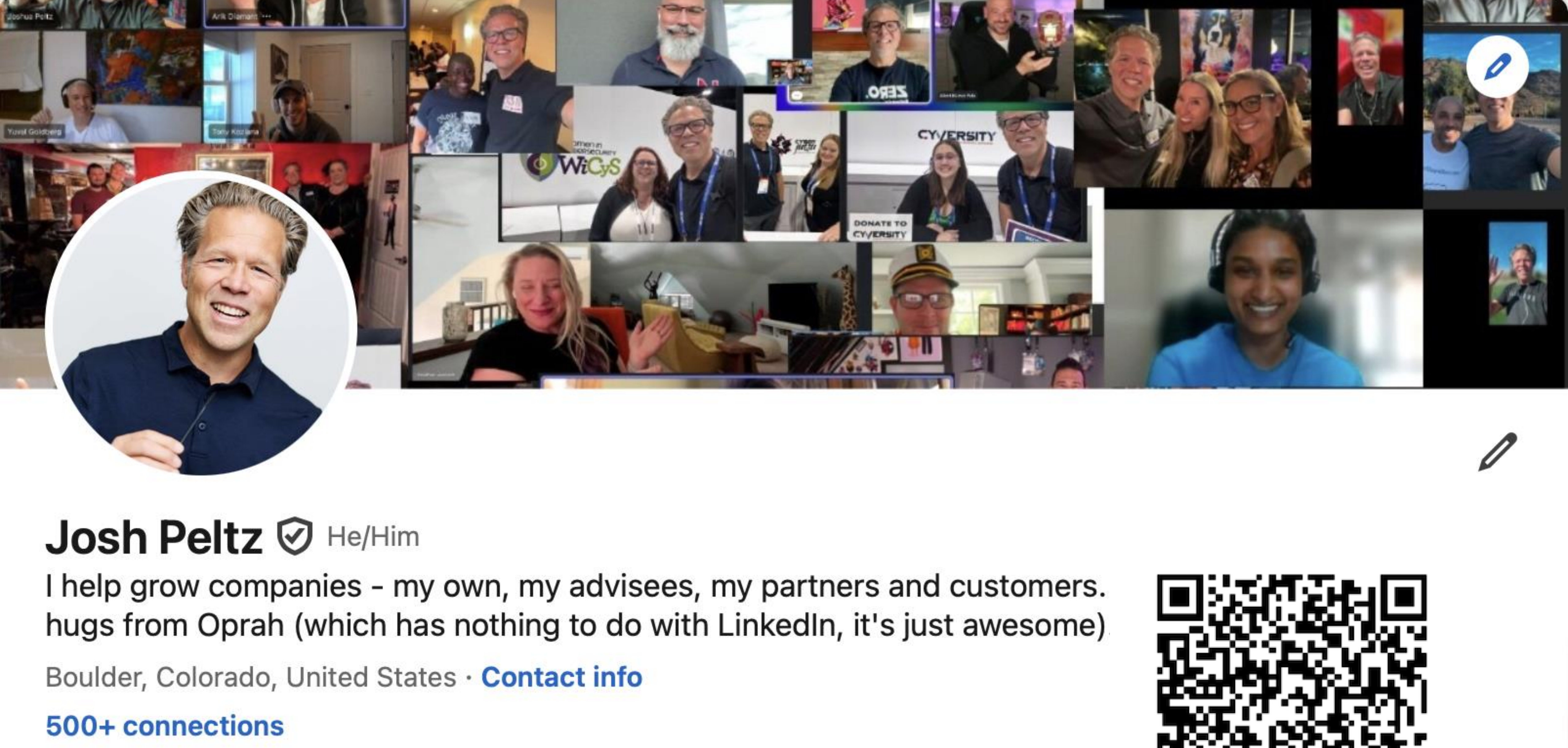
Ever Invite You to Present at CornCon…

on Something Wildly Untested,

Mildly Uncomfortable,

and Totally Brand New for you…

Jump at the Chance!



Josh Peltz He/Him

I help grow companies - my own, my advisees, my partners and customers.
hugs from Oprah (which has nothing to do with LinkedIn, it's just awesome).

Boulder, Colorado, United States · Contact info

500+ connections

Thank You!

My LinkedIn Here →