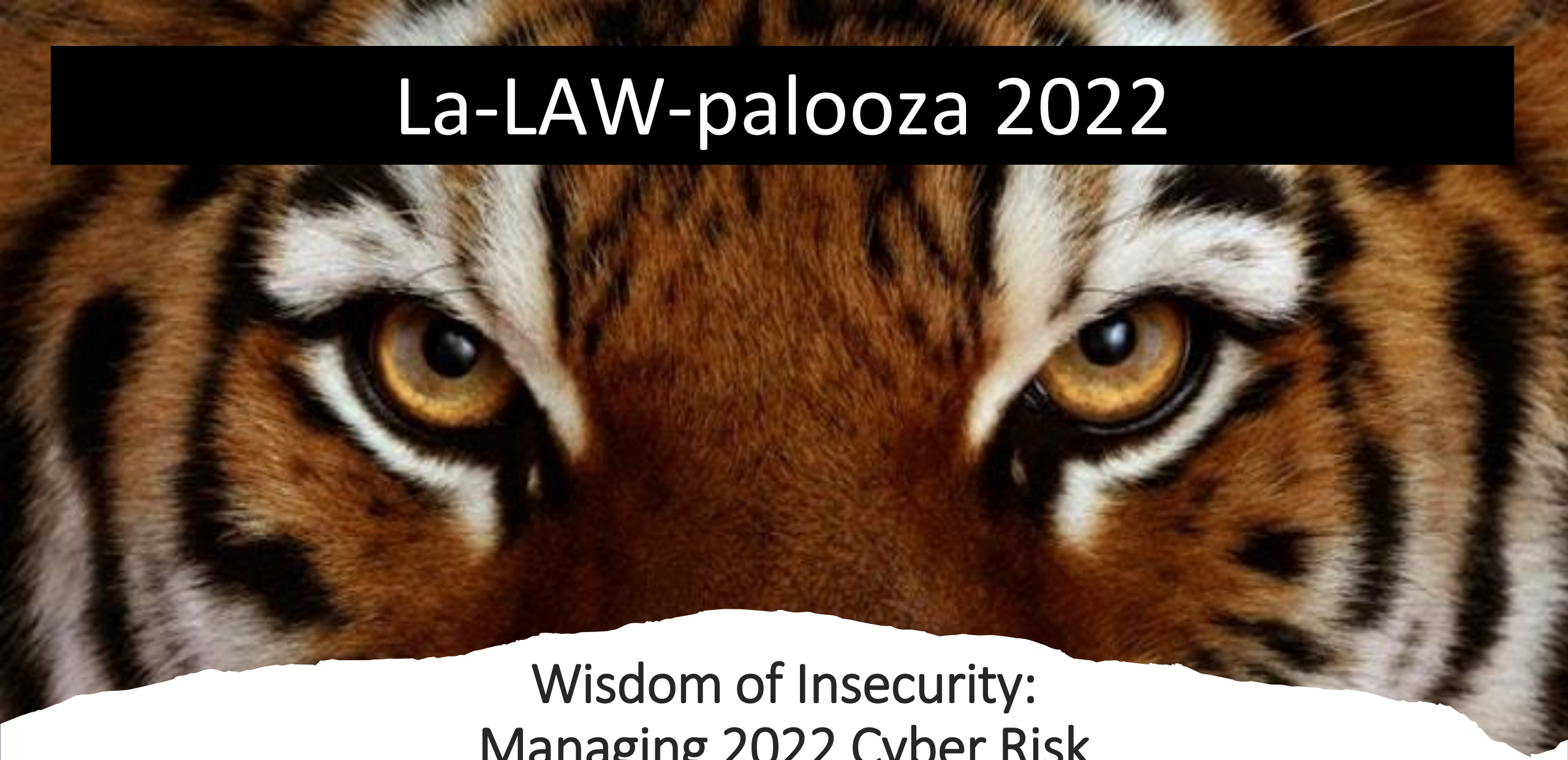


La-LAW-palooza 2022

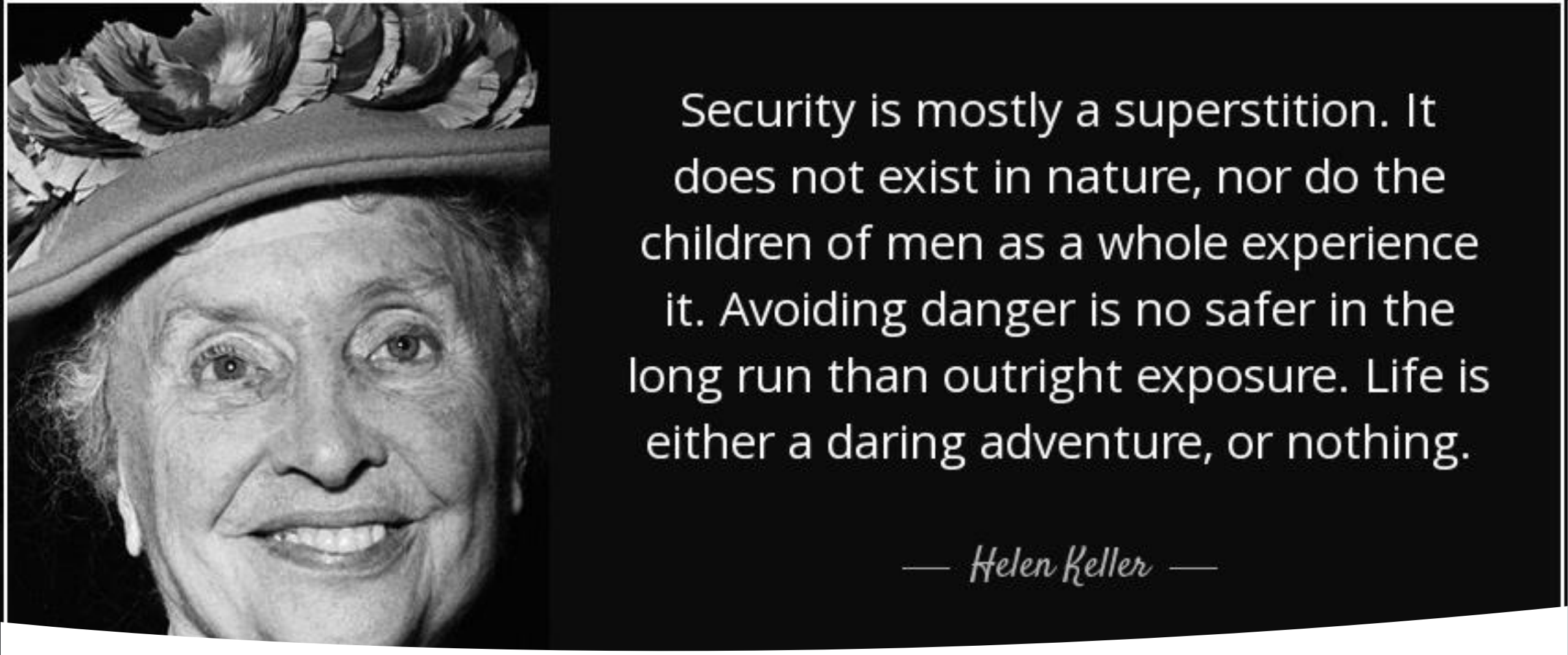
Wisdom of Insecurity: Managing 2022 Cyber Risk

April 26, 2022

Justine Phillips
DLA Piper
Cyber Attorney aka Out-House Counsel

Adam Welland
Altos Labs
VP, Transactions & Partnerships aka In-House Counsel

Your Backstage Cyber Guides



se·cu·ri·ty /səˈkyo͝orədē/
the state of being free from danger or threat

WHO IS THE 2022 TIGER KING?

- Power hungry
- Wants to build an empire
- Paranoid
- Territorial
- Doesn’t play by the rules

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

April 20, 2022 Joint Cyber Advisory

Organizations should immediately implement the following actions to protect against Russian state-sponsored and criminal cyber threats:

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Enforce multifactor authentication.
- Secure and monitor Remote Desktop Protocol and other risky services.
- Provide end-user awareness and training.

Cyber Law Lineup

New Laws & Regulations

- Executive Order on Improving the Nation's Cybersecurity May 12, 2021
- Activated agencies to implement regulations
- FTC, EEOC, DOL, SEC all have new cyber regs
- SEC Regs March 9, 2022
- CPRA goes into effect January 1, 2023
- The Agency enforcing July 1, 2023
- Colorado, Virginia and Utah also have new laws effective in 2023
- Many states in the pipeline

"Real change, enduring change happens one step at a time."

- Ruth Bader Ginsburg

CALIFORNIA CONSUMER PRIVACY ACT: CCPA

- **California Consumer Privacy Act** (Cal. Civ. Code § 1790.100 *et seq*.)
  - Provided privacy rights to consumers and placed obligations on businesses.
  - Gives California Consumers a **private right of action**.
  - CCPA provides **statutory damages of $100-$750** per person, per incident.
  - Businesses have a "**duty** to implement and maintain **reasonable security procedures and practices** appropriate to the nature of the information[.]"

What about the CPRA?

The **California Privacy Rights Act** ("CPRA" or "CCPA 2.0") became law through the passage of Proposition 24 in November 2020 and takes effect in 2023.

- **New Privacy Rights:**
  - Right to Know.
  - Right to Access.
  - Right to Deletion.
  - **Right to Correct**
  - **Right to Opt-out of** Sale or **Sharing.**
  - **Right to Limit Use and Disclosure of Sensitive Personal Information.**
  - Right to Be Free From Retaliation.

- **New Obligations:**
  - Obligation to **retain personal information only as reasonably necessary and proportionate** to achieve the purposes for which the PI was collected and disclose to consumers the retention period.
  - New **contractual obligations for vendors** who access personal information.

What is “Reasonable Security”?

- Reasonable security is defined through an expanding set of laws, regulations, enforcement actions, security frameworks, and common law duties.
- No one size fits all approach.
- Executive Order 14028 – Improving the Nation’s Cybersecurity

No pressure, no diamonds.

Thomas Carlyle

SEC Cyber Focus

Recent Developments

Commission Statement and Guidance on Public Company Cybersecurity Disclosures

October 13, 2011 — February 26, 2018

CF Disclosure Guidance: Topic No. 2 Cybersecurity

SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

March 9, 2022

New Proposed Rules

March 9, 2022

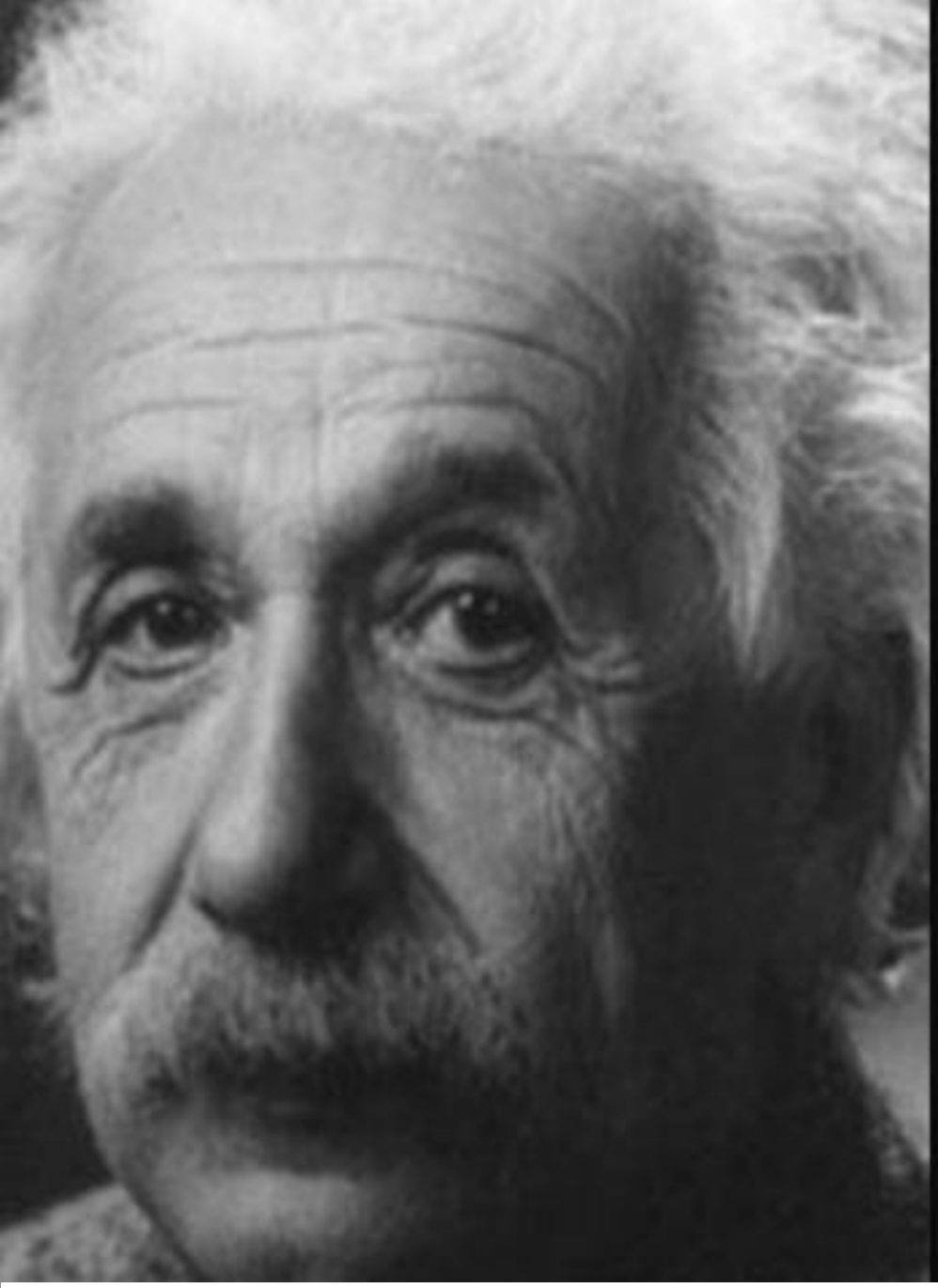
Key requirements:

- File 8-K within 4 business days of determination that the incident is material.
- Provide updates for previously disclosed incidents.
- Disclose information security policies and procedures.
- Disclose cyber risk governance.

Seeking comments by May 9, 2022

What is a Material Cyber Incident?

- The proposed rules will define "**cybersecurity incident**" as an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.
- The proposed rule sets the trigger for disclosure at the determination an incident is material, rather than the date of discovery.
- What is "**material**?"
  - Information is material if there is a substantial likelihood that a reasonable investor would consider it **important in making an investment decision** or if it would have significantly altered the "total mix" of information made available.
  - Material in the **aggregate**



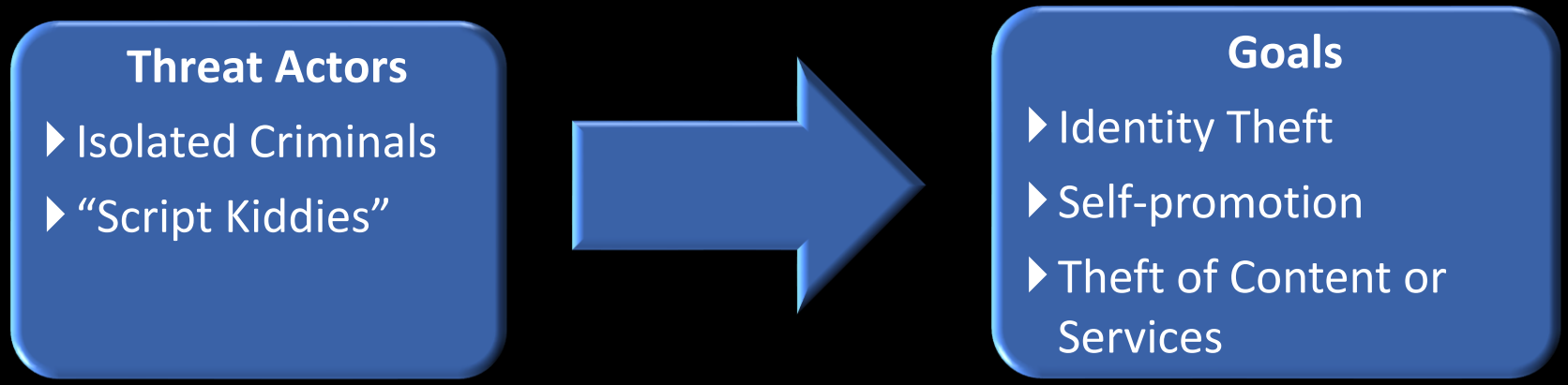
Wisdom is not a product of schooling but of the lifelong attempt to acquire it.

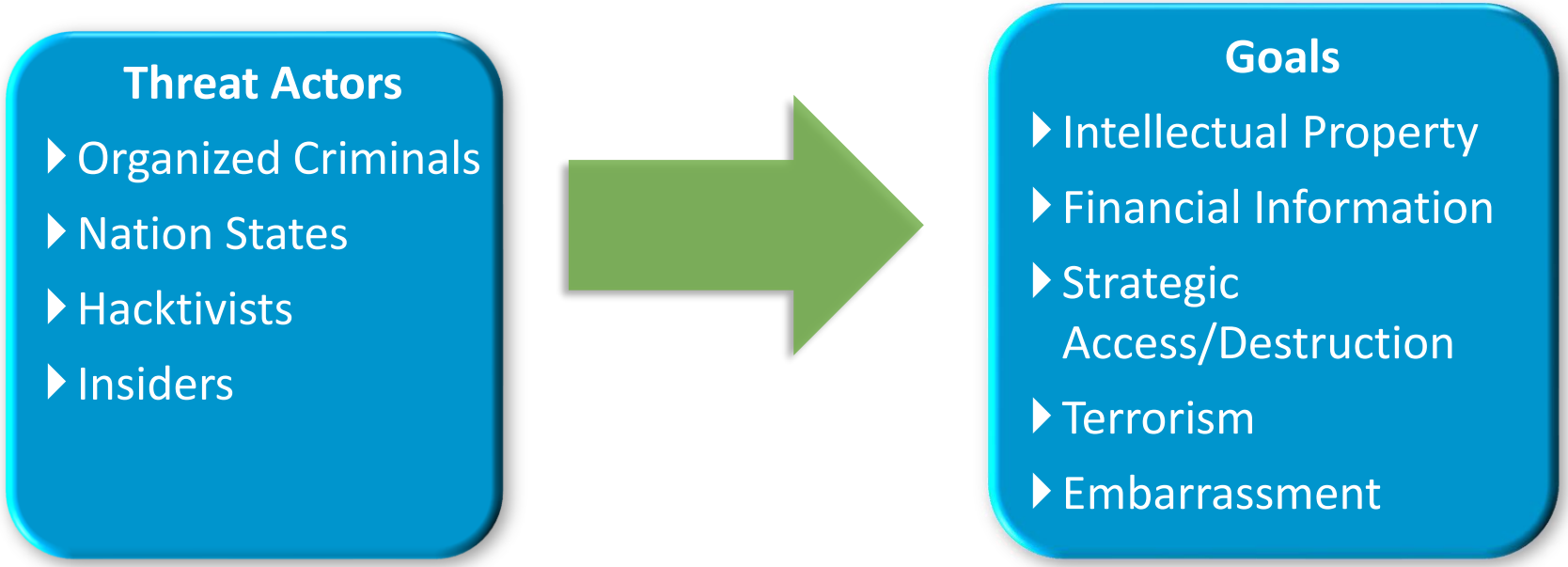
— Albert Einstein —

AZ QUOTES

Understanding the Cyber Threat evolution

Yesterday:





Shifts in Cyber Landscape

1. Cybersecurity spending is at an all-time high and growing

   2012-2019: up 70% / + $62B to **~$150B**
   2019-2028: up 65% / + $98B to **~ $250B**
   Dominated by external spend on managed security services

2. Technological and cyber threats are the number one concern for executives doing business in North America

   3 of the top **5** risks are technology & data driven

3. The frequency and severity of cyber events are increasing rapidly and more sophisticated, with ransomware the biggest threat (according to a DHS CISA advisory on Feb. 9, 2022)

$4.62m

Average total cost of a ransomware breach

Ransomware and destructive attacks were costlier than other types of breaches.

Governing Cyber Risk


Someone's sitting in the shade today because someone planted a tree a long time ago.
-Warren Buffett
QuotesNest.com
www.quotesnest.com

People

(who is doing what?)

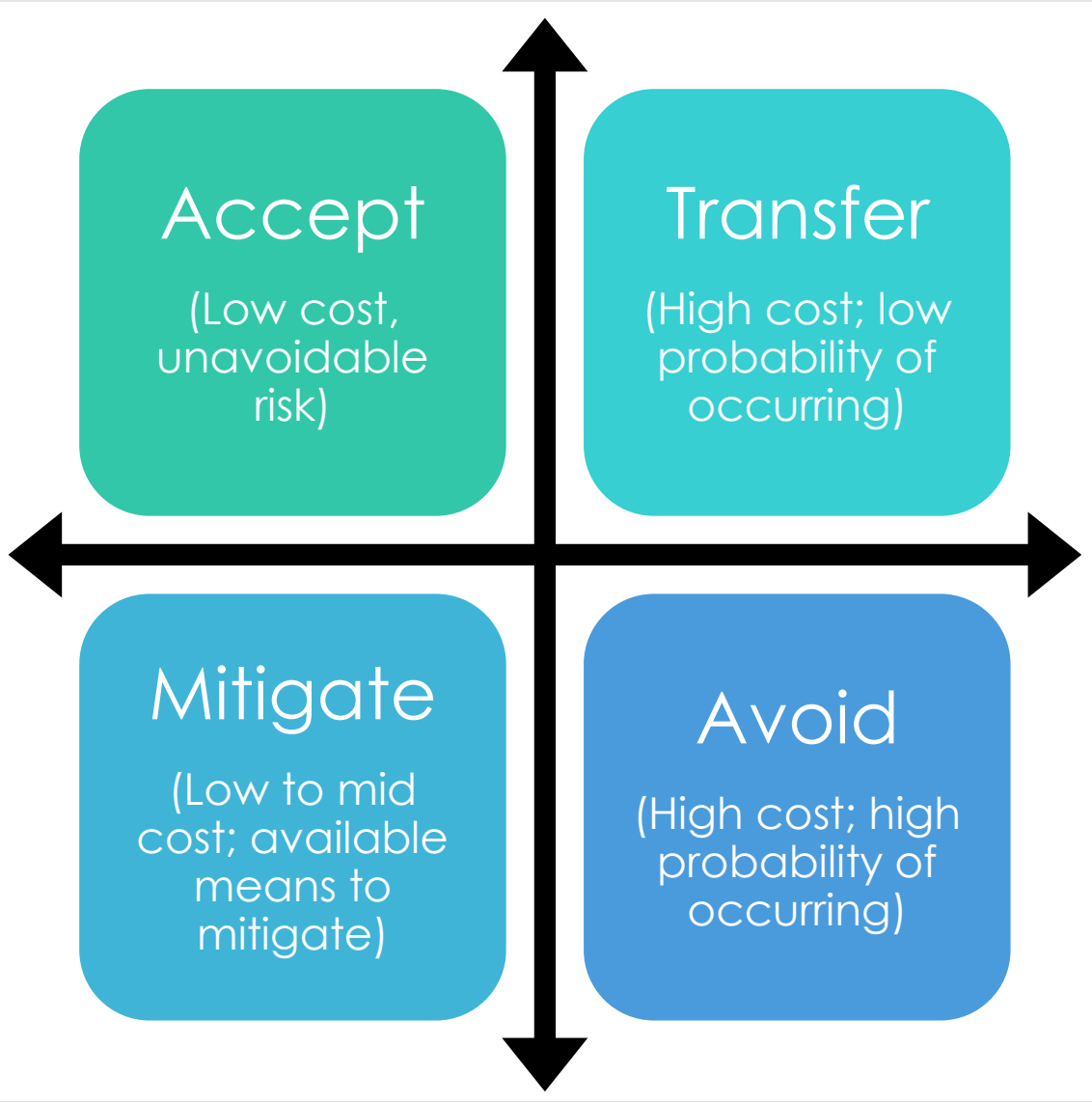
Process

(steps to achieve goals)

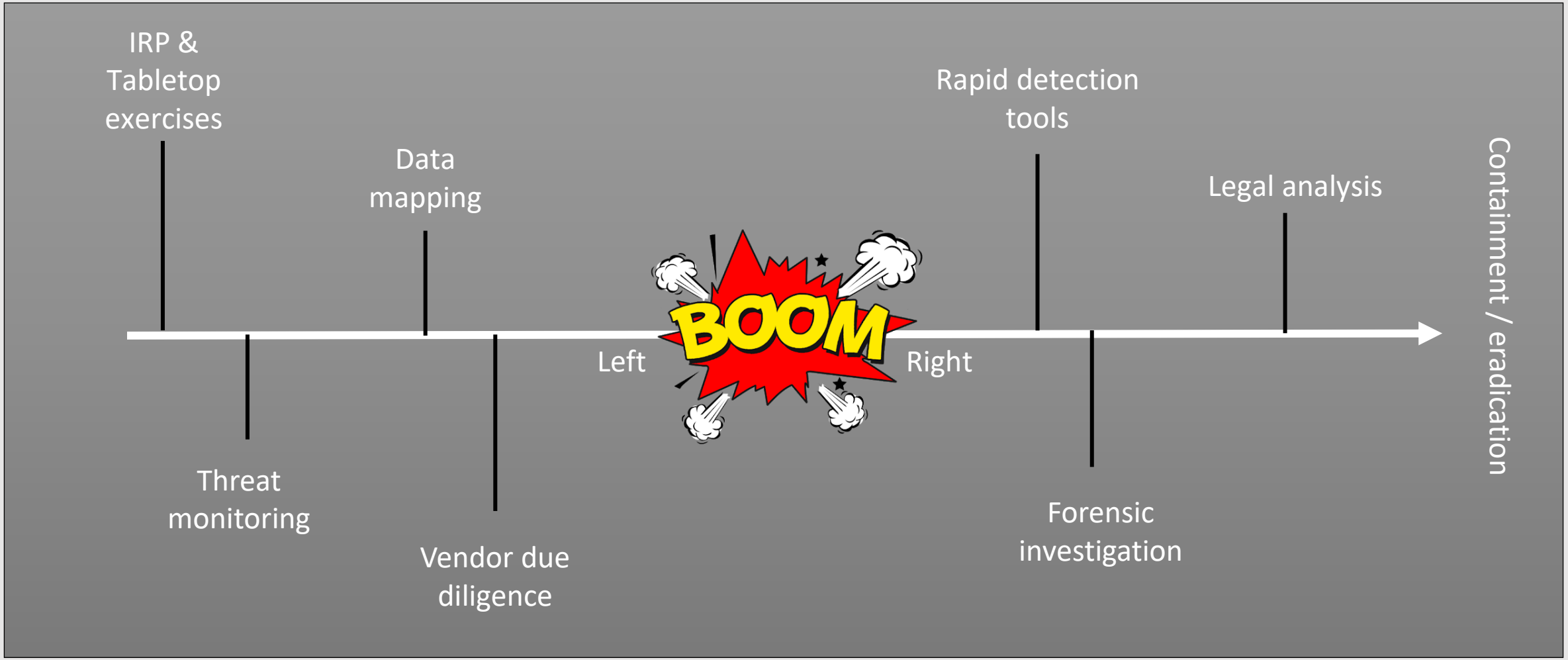
Technology

(tools to increase efficiency)

INFORMATION


Accept
(Low cost, unavoidable risk)
Transfer
(High cost; low probability of occurring)
Mitigate
(Low to mid cost; available means to mitigate)
Avoid
(High cost; high probability of occurring)

Proactive vs. Reactive Risk Management



Defensible Practices

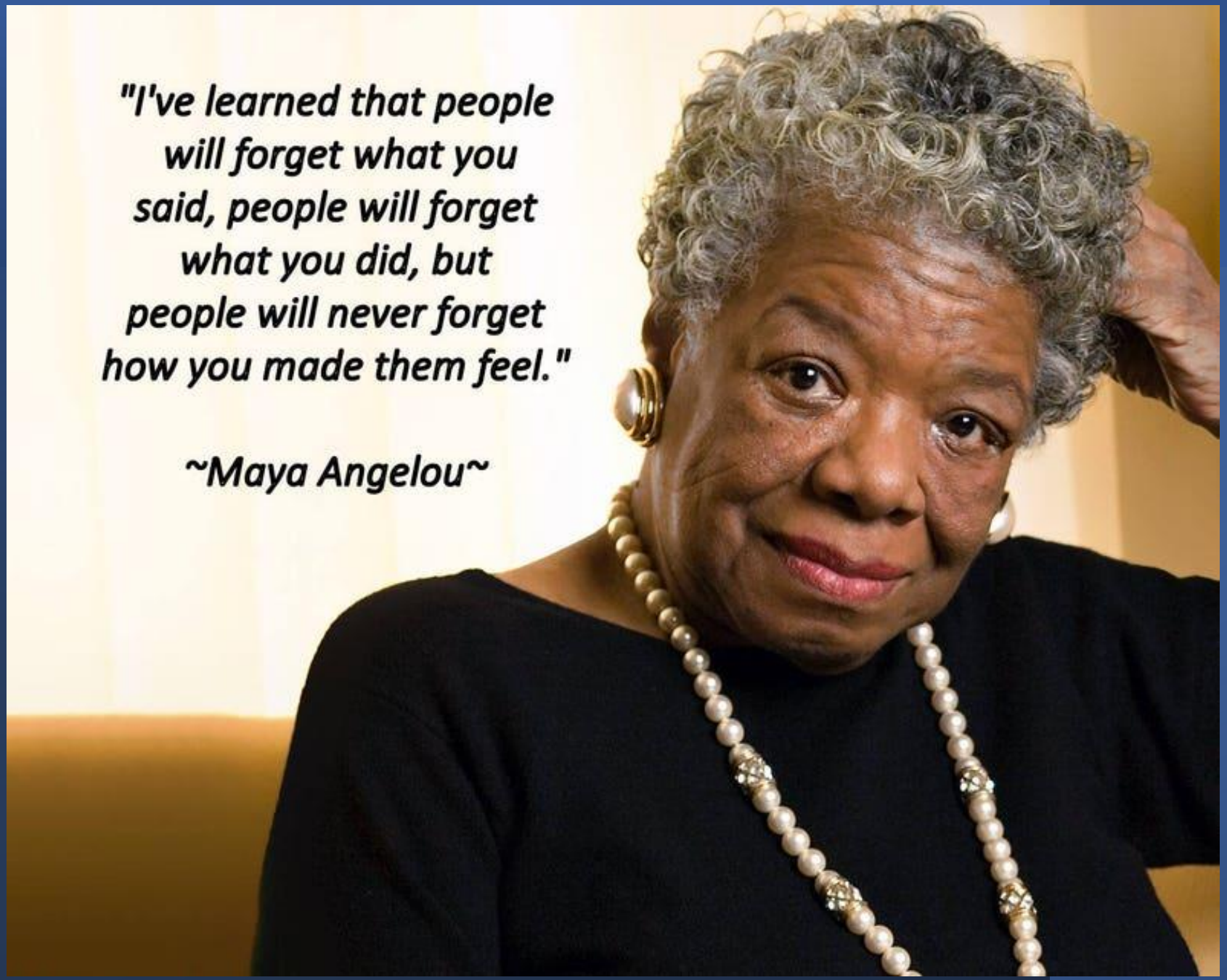
How well did we prepare?

How well did we respond?

Governance Challenges

- Threat actors have more time and more resources
- The threats are constantly changing
- Inadequate information sharing
- Consistently prioritizing cyber risk across the organization
- Chief Information Security Officers cite gaps in skill sets on their teams, lack of bandwidth, and inadequate budgets as some of the biggest issues

Cyber Wisdom:
Seven key principles to governance


"I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel."
~Maya Angelou~

Wise Questions?

Justine Phillips
Cyber Attorney
Data Protection, Privacy, and Security-Regulatory Group
Justine.Phillips@dlapiper.com
(760) 822-3766

Adam Welland
Altos Labs