HaystackID®

False Faces, True Evidence

Unmasking Deepfakes with Digital Forensics

The Masters Conference New York

07 | 22 | 25

The Masters Conference | HAYSTACK®

Panelists

John Wilson

Chief Information Security Officer and President of Forensics

HaystackID

Peter Tsai

Counsel - Litigation

Seyfarth Shaw LLP

Jerry Bui

Founder and CEO

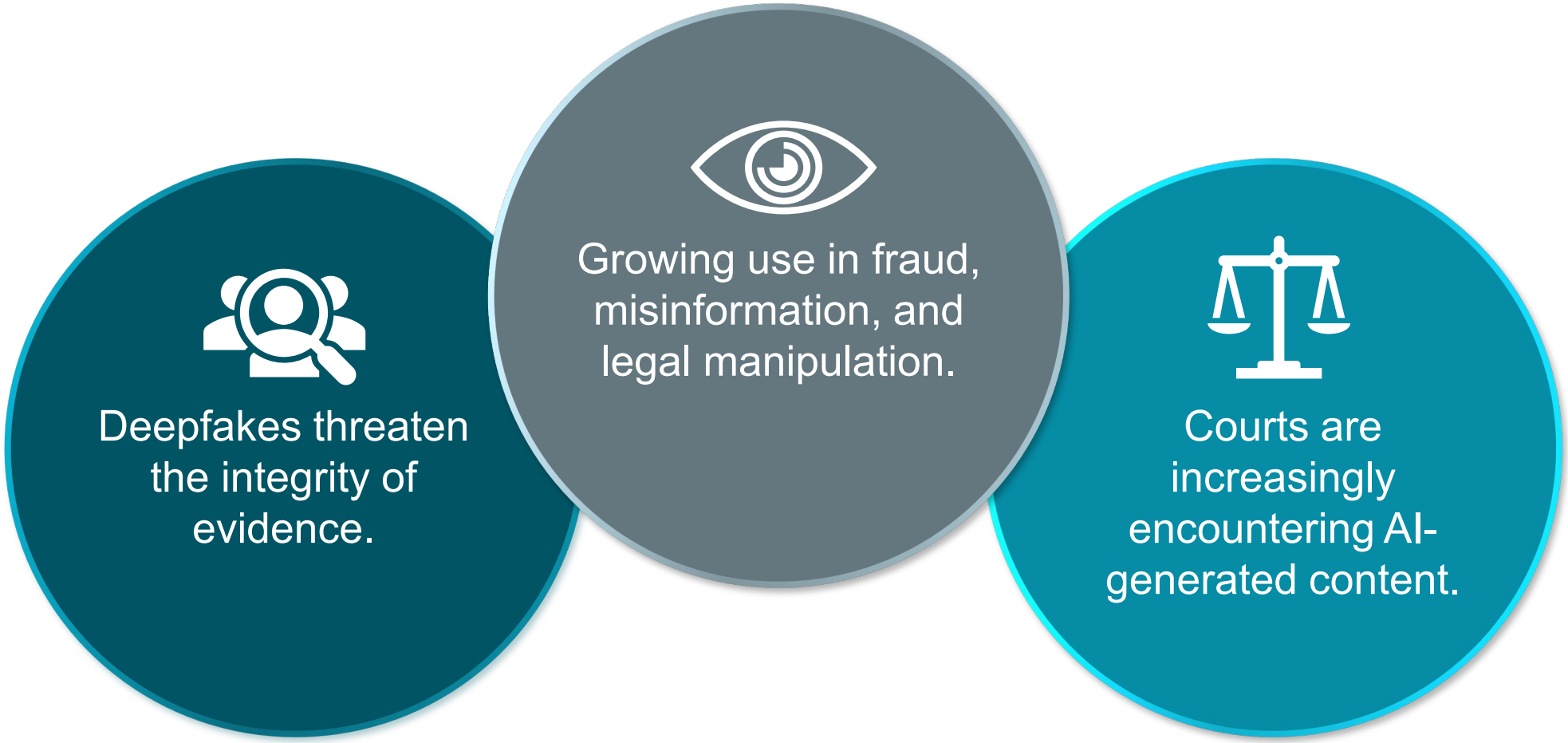
Right Forensics

Alexandria Lutz

Senior Corporate Counsel

Nordstrom, Inc.

Why This Matters to Legal Professionals



What Are Deepfakes?

Synthetic media created using AI (images, video, audio).

Generated by GANs (Generative Adversarial Networks).

Increasingly realistic and accessible.

Real-World Examples

01 Deepfake scam cost UK firm $240K (CEO voice clone).

02 Fake video used in a custody case.

03 False audio in a corporate investigation.

04 Fake board meeting video conference.

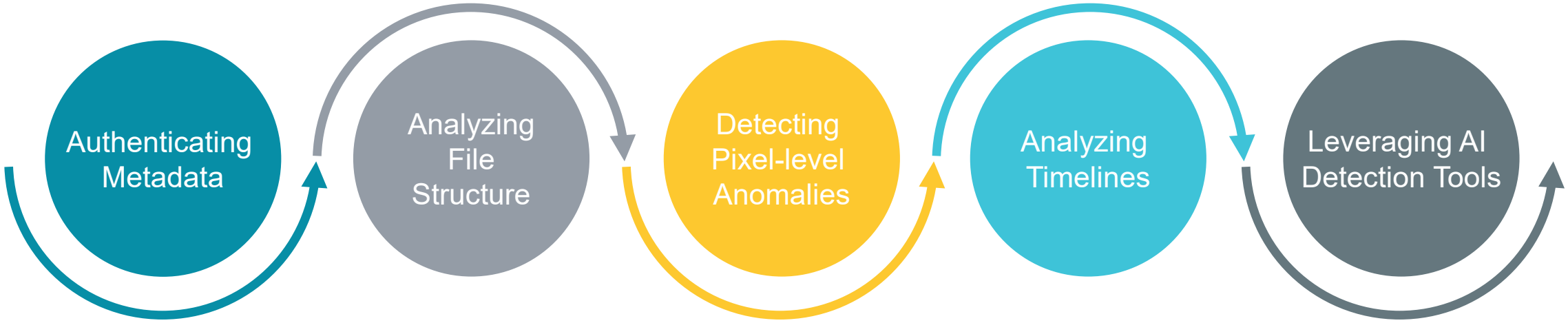
Authenticating Pictures and Videos in State Court

- Authentication of evidence is required before it can be received into evidence. (Evid. Code § 1401.)
- Authentication is the introduction of evidence sufficient to sustain a finding that it is what the proponent claims it is. (Evid. Code § 1400.)
- The burden of proof is on the party offering the evidence. (Evid. Code § 403(a); People v. Lucas (2014) 60 Cal.4th 153, 262.)
- In People v. Beckley (2010), the California Supreme Court emphasized the risks of manipulated digital content, reinforcing the need for reliable authentication methods.

Authenticating Pictures and Videos in State Court (cont.)

- Digital photographs and recordings are classified as “writings” in the Evidence Code, which means they must be “authenticated” before they can be admitted into evidence. (Evidence Code § 250 [recorded statements and photographs are “writings”])
- Who can authenticate photos and videos?
  - The person who took a photograph or video can testify to its authenticity.
  - A witness who has been to the location or seen the object depicted in the photograph or video can testify that the photograph or video truly and accurately represents the location or object.
  - Where no one is qualified to authenticate a photograph or video from personal observation, a photograph or video may be authenticated by the aid of expert testimony. (People v. Beckley (2010) 185 Cal.App.4th 509, 515.)

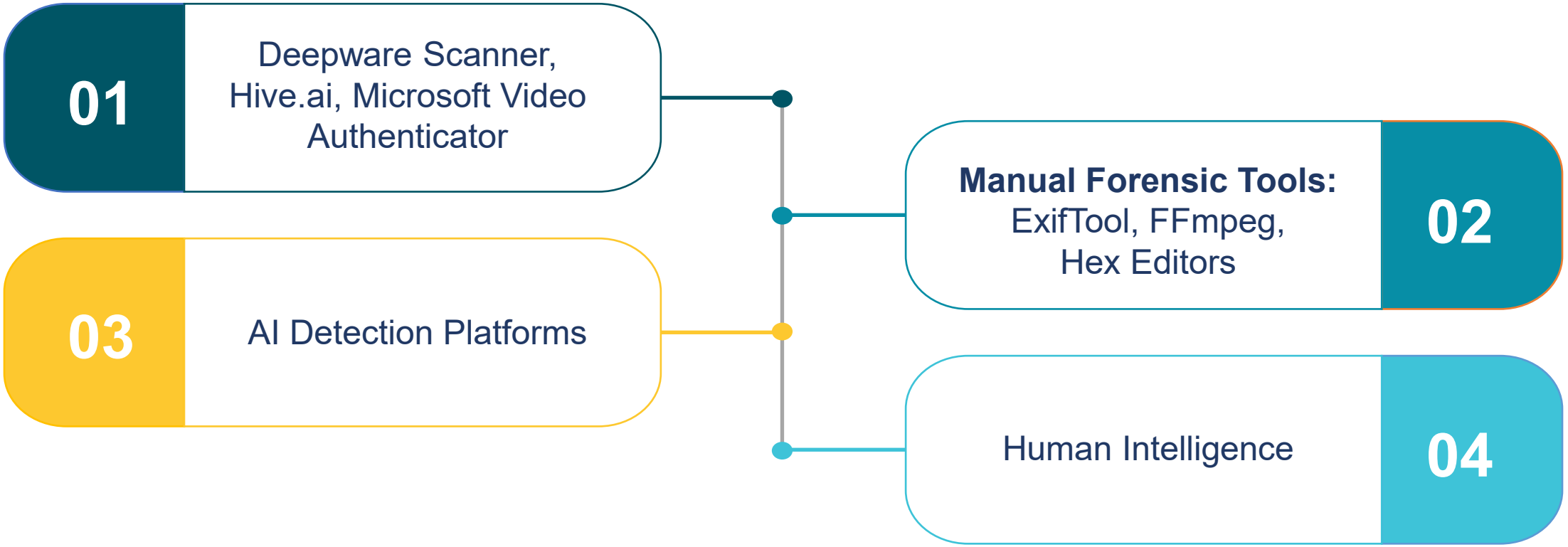
The Forensic Response



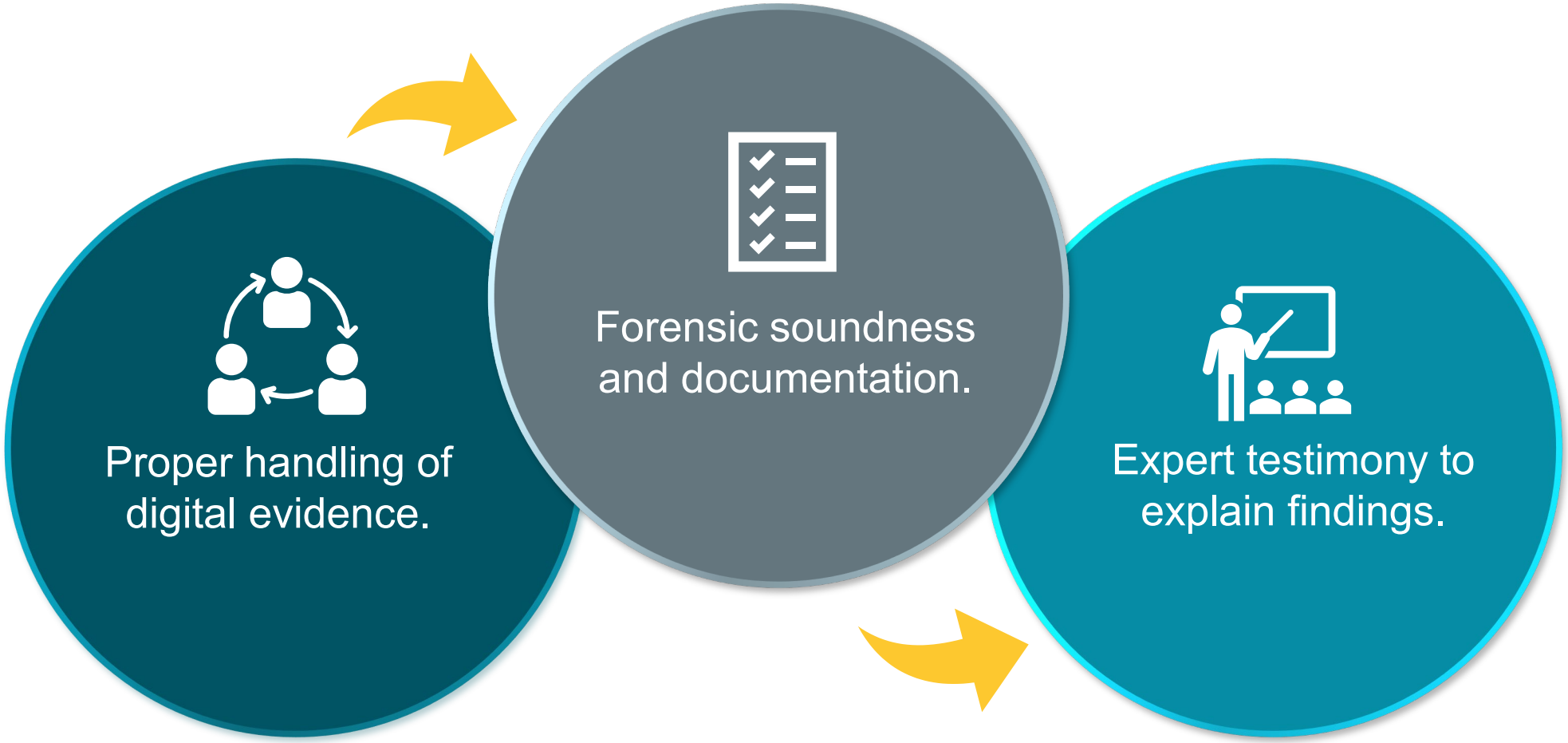
Telltale Signs of Deepfakes

- Inconsistent Lighting and Reflections
- Frame or Lip-sync Mismatch
- Missing Metadata or Strange Encoding
- Audio Artifacts
- Video Artifacts
- ???

Tools of the Trade



Chain of Custody and Admissibility



Case Study 1

Video Manipulation in a Dispute

Allegation:

The video shows an employee breach.

Forensic Analysis:

Revealed frame splicing and mismatched audio.

Result:

Video deemed inadmissible.

Case Study 2

???

Allegation:

Place copy here.

Forensic Analysis:

Place copy here.

Result:

Place copy here.

Deepfake Detection in the Early Stages of eDiscovery

- **Identification:** Speak to your client about the source of the relevant data, assess chain of custody issues, and inquire about any concerns regarding the authenticity of data relevant to the case.
- **Collection:** Consider bringing in a forensic expert to handle the collection of data. In addition to being able to detect any anomalies, the forensic expert can speak to the collection methods and chain of custody if the opposing party calls into question the authenticity of your client's data.
- **Review:** Whether this is data collected from your client or produced by an opposing Party, reviewers should look for the potential red flags. Reviewers should pay close attention to document metadata, such as when the document was modified, what device was used to take a picture, etc.

Practical Detection Steps

Trust

Trust Your Gut

Test

Apply a 3-part Test

- Perfect evidence
- No original copy of the evidence
- Complicated story involving the proffered copy

Verify

Seek a Second Opinion

- Other sources
- More discovery
- Expert analysis

Discovery Strategies to Protect Your Client

- **Requests for Production of Documents:** Request documents in native format with all associated metadata.
- **Utilize Other Written Discovery:** Such as special interrogatories, to gather more facts regarding evidence you suspect may be fabricated.
- **Evidentiary Hearings and Discovery Conferences:** Bring concerns regarding fabricated evidence before the Court as soon as they are identified.
- **Depositions:** Depose witnesses who will testify to the authenticity of the evidence at issue and individuals who have personal knowledge of facts that suggest the evidence may be fabricated.

Questions Legal Teams Should Ask

Where did this media originate?

Has it been altered?

Is metadata intact and credible?

Can it be independently verified?

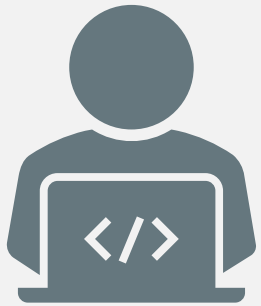
Corporate Reputational Risks

01

Rise of deepfakes increases reputational risk for companies.

02

Threats include impersonation of executives, false endorsements, and fabricated scandals.



03

Speed of misinformation outpaces traditional corporate response timelines.

04

Legal, PR, and cybersecurity teams must align on rapid response protocols.

05

Authenticity and trust are now competitive differentiators.

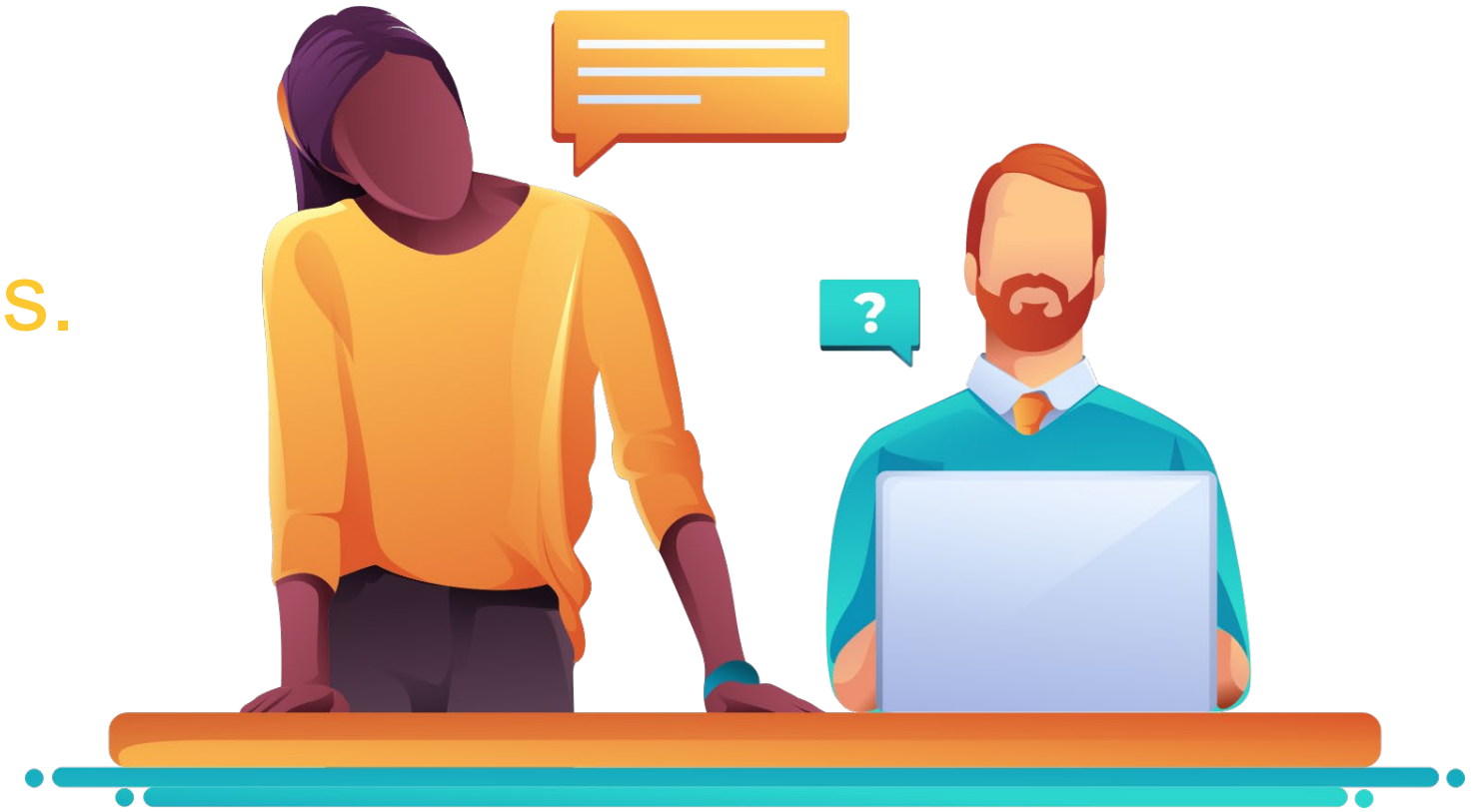
06

Investment in detection, training, and proactive monitoring is essential.

Summary and Key Takeaways

Q&A

Let’s discuss your questions and experiences.



Resources and Contacts

Recommended Tools and Reading List:

- Article 1
- Article 2
- Article 3
- Article 4

Contacts:

- John Wilson
- Peter Tsai
- Jerry Bui
- Alexandria Lutz

Questions?

Learn more at HaystackID.com
or reach out to us at Info@HaystackID.com / 800.267.9695

The Masters Conference | HAYSTACK®