Digital incident & litigation response playbook

Friday, 13 September
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST

iapp

Welcomes and Introductions

Panelists

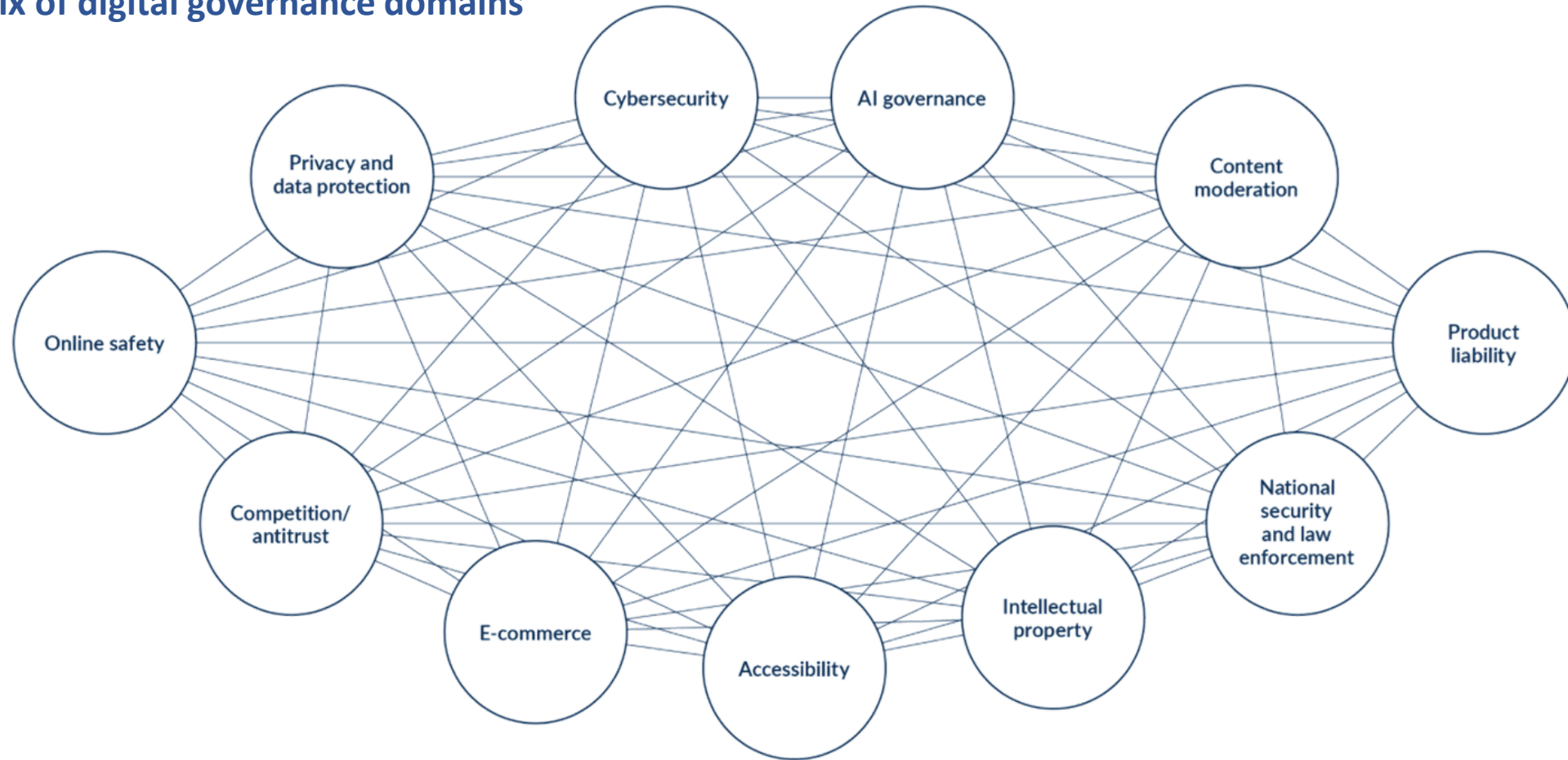**Caitlin Fennessy**
VP & Chief Knowledge Officer
IAPP

Fred H. Cate
Distinguished Professor, Indiana
University Maurer School of Law
Senior Advisor, Red Barn Strategy

Stanley W. Crosley
Managing Partner
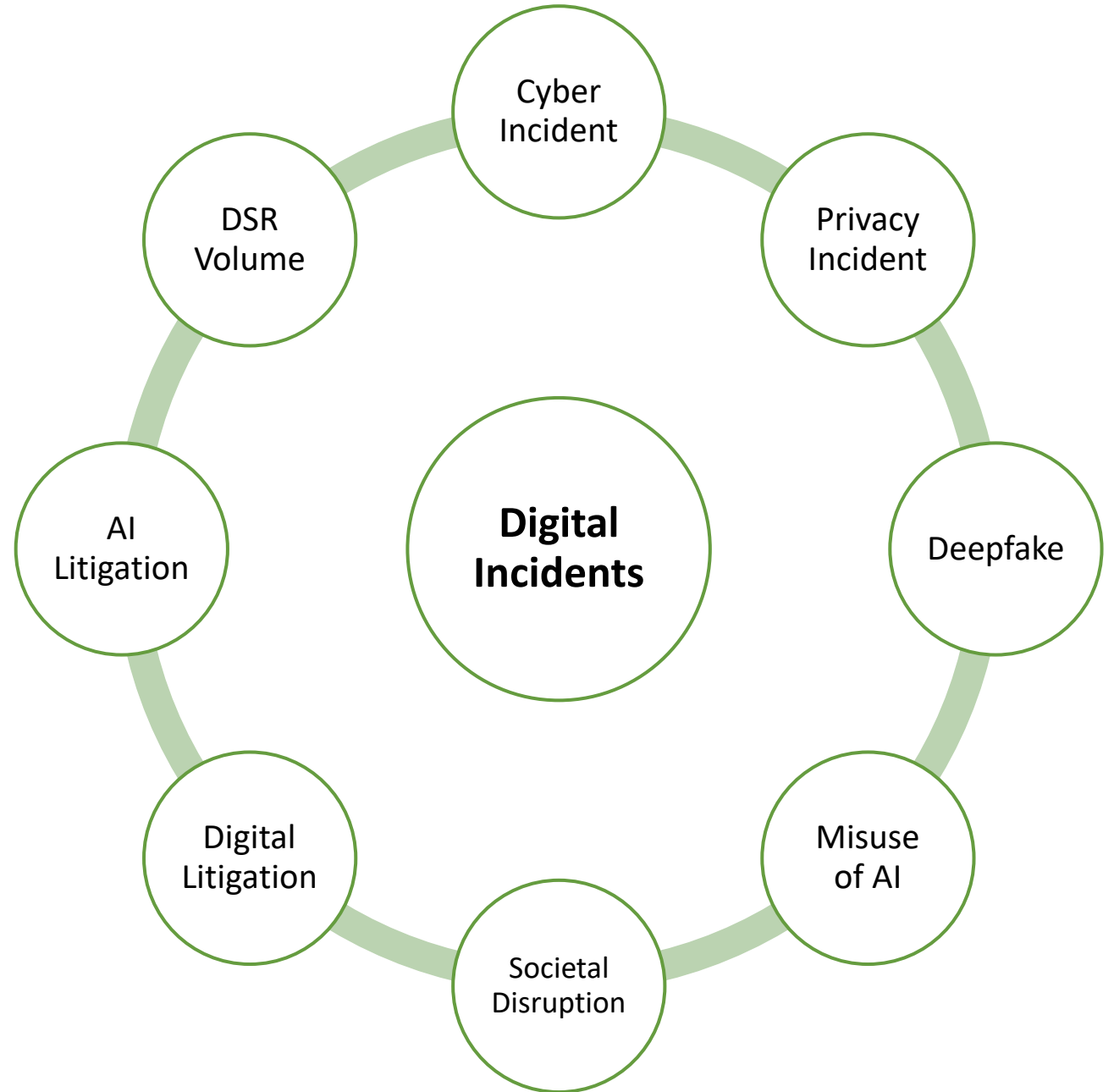Crosley Law Offices &
Red Barn Strategy

IAPP's Organizational Digital Governance Report

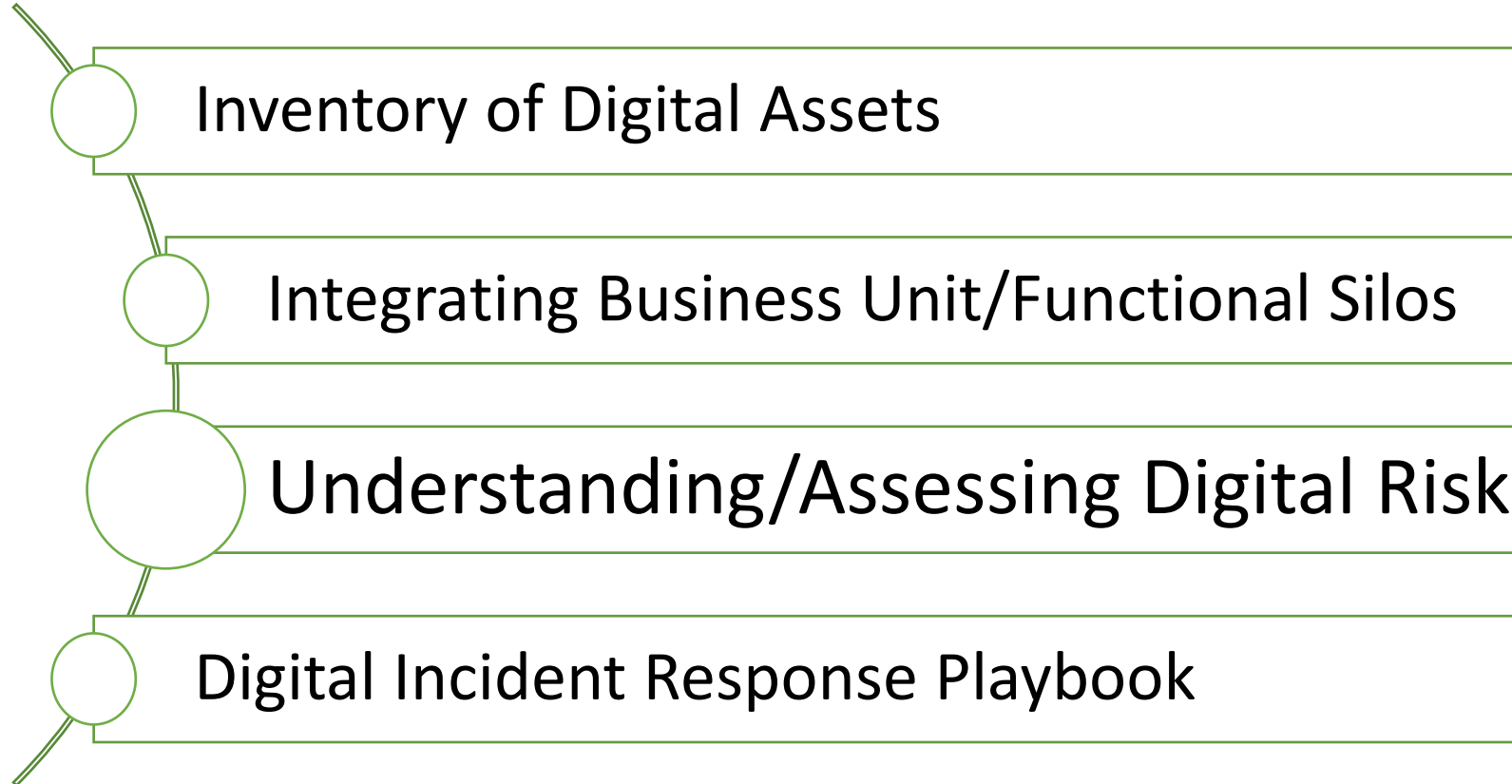**Matrix of digital governance domains**

Digital Incidents

- Expansion of incident types and scope of incident response planning

- Traditional and non-traditional attack vectors

- Need for cross-functional coordination

Cyber Incident

DSR Volume

Privacy Incident

AI Litigation

Digital Incidents

Deepfake

Digital Litigation

Misuse of AI

Societal Disruption

Digital Incident Response Planning: *Digital Governance*

Inventory of Digital Assets

Integrating Business Unit/Functional Silos

Understanding/Assessing Digital Risk
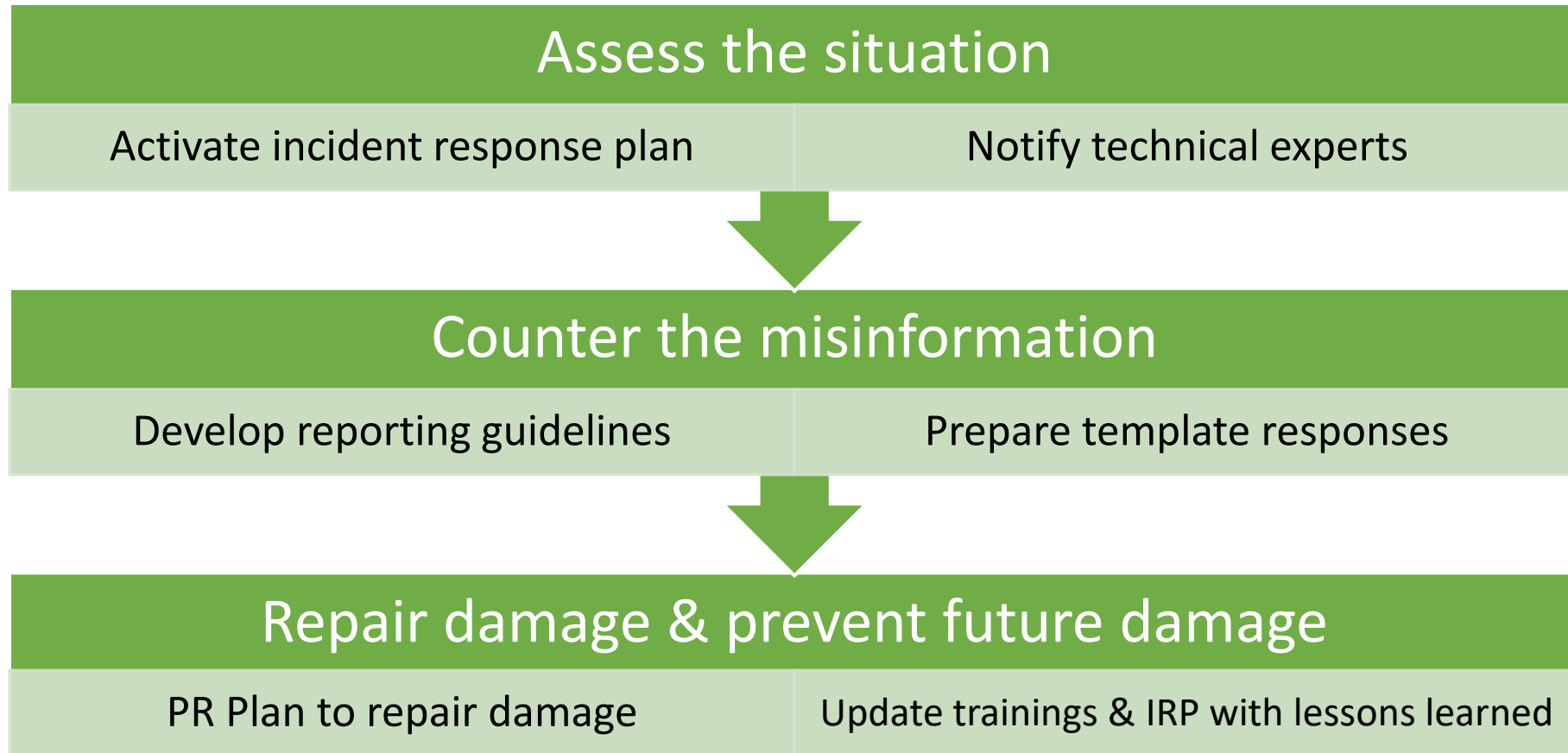
Digital Incident Response Playbook

Creating a Digital Incident Playbook

- Expansion of Incident Response Plan
  - Cover scope of digital incidents
  - Contact information and key templates

- Key internal players & contact information
  - Who has technical knowledge to understand the event?
  - Who is on the digital incident response team? Who leads?

- Key external players
  - Insurance, forensic investigators, outside counsel
  - Who is responsible for contacting?

Incident Highlight: Deepfakes

- Deepfake Technology Risks
  - Spear-phishing precision with generative AI
    - Communications to employees/customers
  - Spoofing biometrics for access to systems
  - DeepFake of Executives/Stakeholders

- Preparing for a Potential Deepfake Incident
  - Understand and align on what is "normal" and "culturally consistent"
  - Designate incident response team and point person
  - Identify and coordinate with vendors and external contacts – expertise is hard to find
  - Integrate deepfake considerations into current IRP

Incident Highlight: Deepfake Response

Assess the situation

| Activate incident response plan | Notify technical experts |

Counter the misinformation

| Develop reporting guidelines | Prepare template responses |

Repair damage & prevent future damage

| PR Plan to repair damage | Update trainings & IRP with lessons learned |

Incident Highlight: Digital Litigation

- Wave of plaintiff litigation using laws with a PRA
  - Unique type of litigation – not product liability
  - Creative application of federal laws such as ECPA and VPPA
  - State laws such as CA CIPA, CMIA, CCPA
  - Expertise in these laws is not usually core to most companies – who interprets?

- Key steps for preparation
  - Assign internal authority for laws
  - Conduct Digital asset inventory for websites and mobile apps
  - Understand technologies used (cookies/pixels/SDKs) and data collected and 3rd parties involved, nature of contracts (clickwrap?)
  - Know the technical players: who codes the sites?

- Trainings and awareness
  - Notify litigation teams of digital (and AI) litigation trends
  - Notify and train IT and marketing teams

Challenges of Digital Incident Response Planning

- Identifying individuals or vendors with relevant expertise
- Cross-functional coordination of teams
- Sustaining training and awareness as the landscape changes
- Keeping up with the rapidly changing landscape
  - Technical capabilities of AI and other emerging tech
  - Business models and creativity of teams
  - Laws and regulations impacting digital governance
  - Societal expectations

Questions and Answers

Panelists

Caitlin Fennessy
VP & Chief Knowledge Officer
IAPP

Fred H. Cate
Senior Advisor, Red Barn Strategy
Distinguished Professor, Indiana
University Maurer School of Law

Stanley W. Crosley
Managing Partner
Crosley Law Offices &
Red Barn Strategy

Resources

- Crosley Law Offices

- IAPP's Organizational Digital Governance Report 2024

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/ACtQeZ3ckP

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:
  This IAPP web conference may be applied toward the continuing privacy education
  (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM
  credential worth 1.0 credit hour. IAPP-certified professionals who are the named
  participant of the registration will automatically receive credit. If another certified
  professional has participated in the program but is not the named participant then
  the individual may submit for credit by submitting the continuing education
  application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:
  The IAPP provides certificates of attendance to web conference attendees.
  Certificates must be self-submitted to the appropriate jurisdiction for
  continuing education credits. Please consult your specific governing body's
  rules and regulations to confirm if a web conference is an eligible format
  for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of
  programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation
please contact: **livewebconteam@iapp.org**