

RSA[®]Conference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: LAW-M03

The State(s) of Cyber Incentives- Creative Laws Driving Better Security



MODERATOR: **Brian Ray**

Professor and Director, Center for Cybersecurity & Privacy, Cleveland-Marshall College of Law

PANELISTS: **Kirk Herath**

Director, Cyber Ohio

Tony Sager

Senior Vice President and Chief
Evangelist, Center for Internet
Security
@cisecurity

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Ohio Data Protection Act

Legal Safe Harbor

Affirmative defense to a cause of action sounding in tort related to data breach

Applies to all businesses that implement a cybersecurity program that complies with specified regulatory frameworks found in the statute

Business Incentive

Acts as an incentive to encourage cybersecurity within the business community

DOES NOT create a minimum cybersecurity standard or private of action

NIST Cybersecurity Framework, 800-53, 53A, or 800-171

Federal Risk and Authorization Management Program (FEDRAMP)

Center for Internet Security Critical Security Controls (CIS CSC)

ISO/IEC 27000 Family

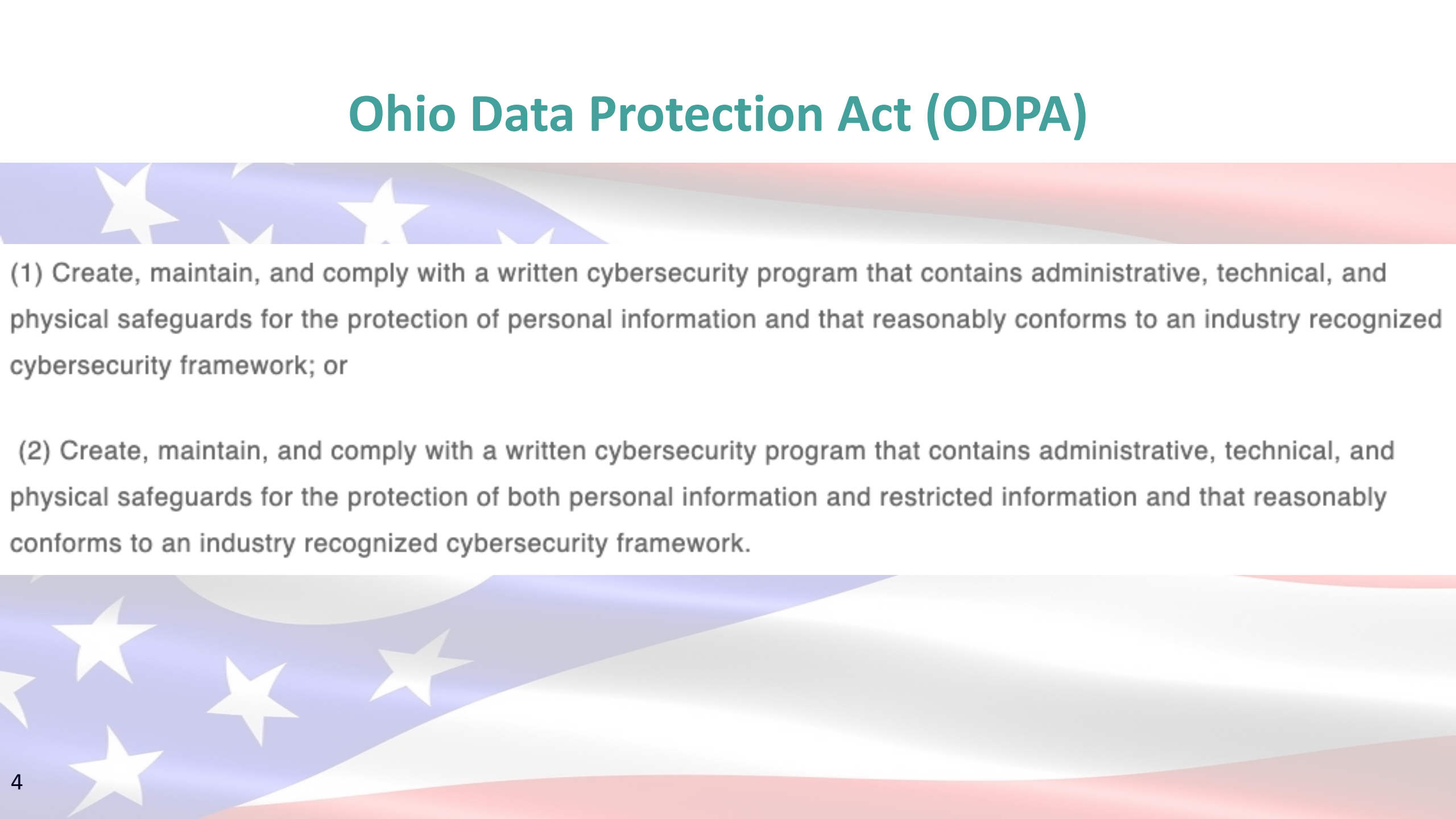
HIPAA Security Rule Subpart C or HITECH

GLBA Title V

Federal Information Security Modernization (FISMA)

Payment Card Industry standard (PCI) plus another listed framework

Ohio Data Protection Act (ODPA)

- 
- The background of the slide features a stylized American flag with white stars on a blue field and red and white stripes, waving across the entire page.
- (1) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework; or
 - (2) Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry recognized cybersecurity framework.

Connecticut Public Act No. 21-119

An Act Incentivizing the Adoption of Cybersecurity Standards for Business--AKA
The Cybersecurity Standards Act



- Two Assumptions:
 - Cybersecurity is largely VOLUNTARY; and
 - Political non-starter to create a statutory minimum standard of
- Conclusion: we need to INCENTIVIZE the voluntary adoption of cyber best practices

Connecticut's Cybersecurity Standards Act

- Clear requirements to EARN incentive:
 - (A) Protect the security and confidentiality of such information;
 - (B) Protect against any threats or hazards to the security or integrity of such information; and
 - (C) Protect against unauthorized access to and acquisition of the information that would result in a material risk of identity theft.
- Flexible scale and scope:
 - (A) The size and complexity of the covered entity;
 - (B) the nature and scope of the activities of the covered entity;
 - (C) the sensitivity of the information to be protected; and
 - (D) the cost and availability of tools to improve information security and reduce vulnerabilities
- Industry frameworks for guidance:
 - The NIST framework, codified by Congress; and
 - The CIS Critical Security Controls, being adopted by industry (e.g., the Defense & Aerospace Industry; several U.S. states (e.g., Ohio & Utah); and around the world.

Benefits and Challenges of Incentive-Based Cybersecurity Laws

- What are the advantages/disadvantages of an incentive-based approach vs a mandatory law?
- How does the incorporation of risk frameworks like the CIS controls help organizations develop a practical and defensibly “reasonable” cybersecurity program?
- Can small businesses implement “compliant” programs?

A Security Framework or Program should *help* you

- How do I choose the most effective actions (based on data)?
- How do I get started? Is there an “on ramp”?
- How do I prioritize action?
- How do I measure progress; how do I compare to others?
- What value is there in what I already own (and do)?
- How do I learn from others? Where can I get training?
- How much can I automate?
- What vendors support this? How can I be sure?
- How does this relate to other frameworks?

Hypotheticals

- Cloud-based business based OH seeks advice on “complying” with the ODPA using CIS framework.
- Same business experiences a data breach resulting from a vulnerability that was identified as low risk during the risk assessment process. What happens under the ODPA? CT?
- Same business experiences a data breach resulting from a failure to adhere to the security program it developed. What happens under the ODPA? CT?

RSA[®]Conference2022

MODERATOR:

Brian Ray

Professor and Director, Center for
Cybersecurity & Privacy
Cleveland-Marshall College of
Law

PANELISTS:

Kirk Herath

Director
CyberOhio

Tony Sager

Senior Vice President and Chief Evangelist, Center for
Internet Security
@cisecurity

