Chief Information Security Officers

BEST PRACTICES ROUND TABLE

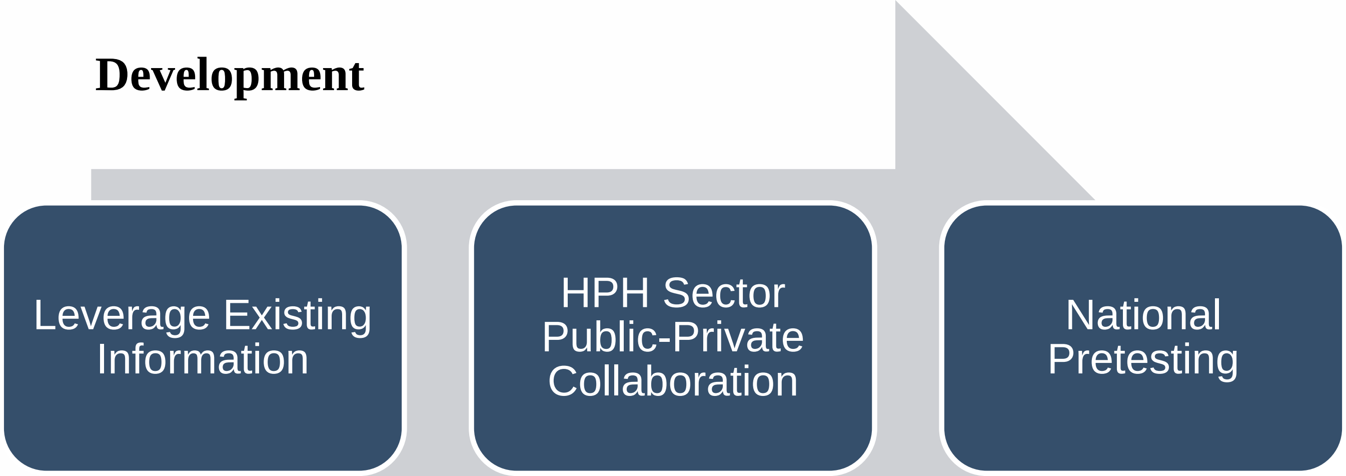
28th National HIPAA Summit

Document Objective and Development

Objective

The CSA 405(d) document aims to raise awareness, provide vetted practices, and foster consistency in mitigating the most pertinent and current cybersecurity threats to the sector. It seeks to aid the HPH sector organizations to develop meaningful cybersecurity objectives and outcomes.

Development



Leverage Existing Information

HPH Sector Public-Private Collaboration

National Pretesting

Existing information and guidance (e.g., NIST Cybersecurity Framework) was leveraged across the public and private domains to provide a tailored approach for the healthcare industry. It does not create new frameworks, re-write specifications, or "reinvent the wheel."

To ensure a successful outcome and a collaborative process, HHS reached out to a diverse set of healthcare and cybersecurity experts from the public and private sectors. Participation is open and voluntary.

Document - Content Overview (1/2)

After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.
- *Technical Volume 1* discusses these ten cybersecurity practices for **small** healthcare organizations.
- *Technical Volume 2* discusses these ten cybersecurity practices for **medium and large** healthcare organizations.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.

The **5 current threats** identified in healthcare:

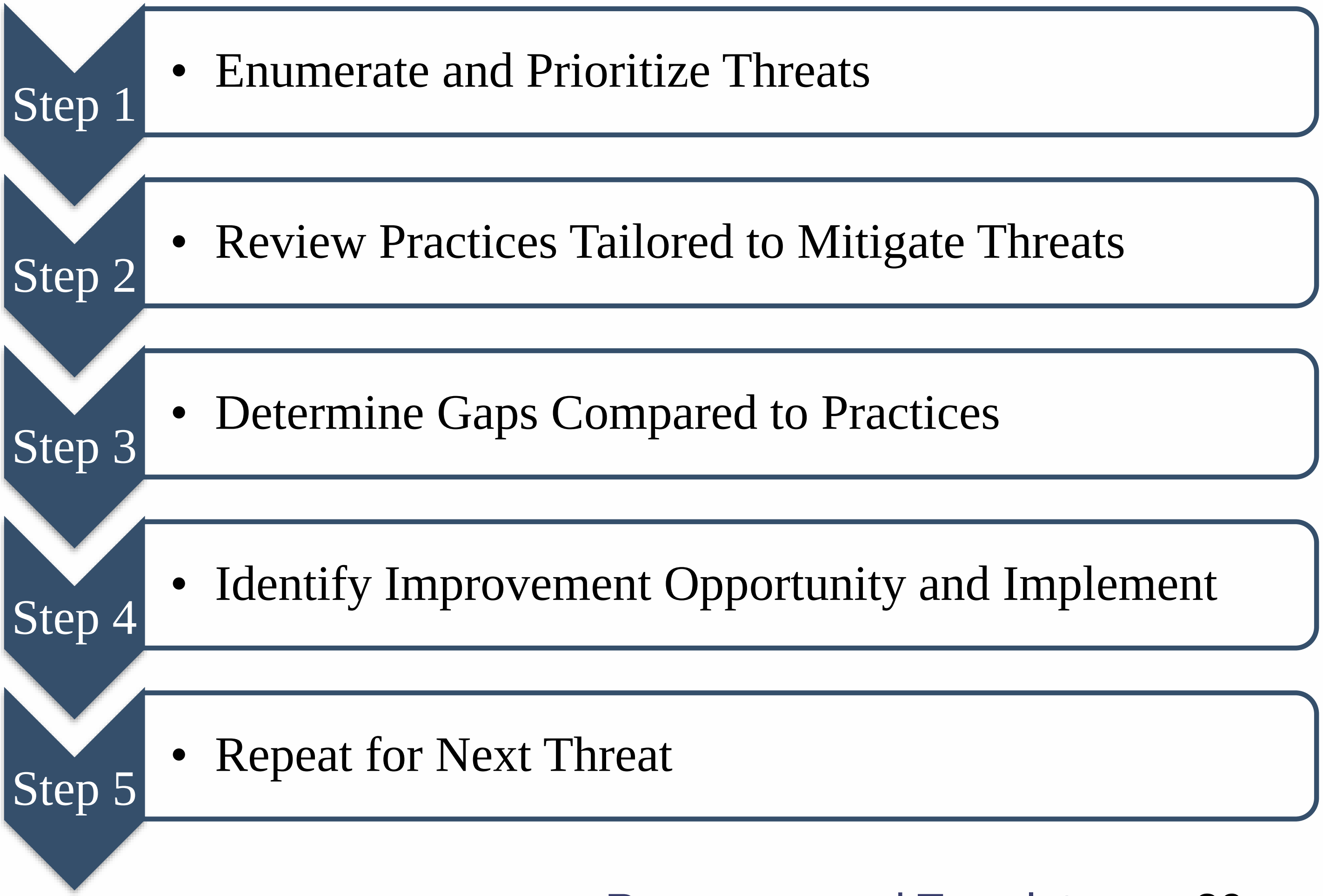
1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data
4. Internal, Accidental, or Intentional Data Loss
5. Attacks Against Connected Medical Devices that May Affect Patient Safety

Document - Content Overview (2/2)

The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Suggested Assessment Process



Step 1
- Enumerate and Prioritize Threats

Step 2
- Review Practices Tailored to Mitigate Threats

Step 3
- Determine Gaps Compared to Practices

Step 4
- Identify Improvement Opportunity and Implement

Step 5
- Repeat for Next Threat

Resources and Templates, p. 39