The Risk of Propagating Standards

Matt Bishop
Dept. of Computer Science, UC Davis

Candice Hoke
School of Law, Cleveland State University

1

Thesis

- Guidance documents make assumptions about the environment to which they are applied
- These assumptions may be *implicit* and therefore the appliers not aware of them
- The guidance documents may not state their recommendations in language (or concepts) that the appliers understand

2

Example

- In U.S., local governments usually lack resources (people) the federal (national) government has
  - So standards written for federal agencies assume resources (people) not available to state agencies
  - Different environment: local governments may have less control over systems than the federal government requires

3

Risk #1

"Best practices" and operational standards make assumptions about the resources available to organizations, and how organizations work, without stating these assumptions explicitly. This leads to an erroneous perception of universal applicability of the "best practices" and standards.

4

Example

- Apply a consensus-driven benchmark to a university computer and find it is non-secure
  - Benchmark minimizes sharing, access
  - Appropriate for businesses but not universities
- Benchmark did not state target environment

5

Use of PKI

- Use of SSL/TLS requires supporting public key infrastructure (PKI)
  - Raises huge issues of trust, credibility of certificates and certificate issuers
  - If not understood, could lead to reliance on:
    - Invalid certificates (it's expired)
    - Untrustworthy certificates (issuer's standards don't match what is needed or expected)

6

Risk #2

"Best practices" and operational standards are written for a particular audience, but the *actual* users of that guidance may be a very different audience for whom the guidance is not understood or (worse) misinterpreted.

7

Example

- Guidance document requires web clients to run Java scripts
  - Implication: don't use Chrome on the Mac for this

8

Risk #3

"Best practices" and operational standards make assumptions about the technology and management in which they are implemented and used, often without stating those assumptions explicitly.

9

Example

- Are these concerns *really* problems?
- No data about:
  - Whether these "gaps" in understanding exist
  - How broad they are
  - How consequential they are

10

Risk #4

Lack of data on the *actual practice* of cybersecurity undermines claims of effectiveness of cybersecurity mandates and ability to handle attacks.

11

Conclusion

- Ultimate risk: governments and organizations may lack the expertise to implement standards and best practices effectively, or may apply them in situations where some components should not be applied
  - A security-motivated organization may rely on omnibus guidance documents that are not well-designed for that organization's context . . .
  - And thereby unintentionally weaken their security

12

Thank you!

- Questions?
- Answers?
- . . .