Compliance Cautions

INVESTIGATING SECURITY ISSUES ASSOCIATED WITH U.S. DIGITAL-SECURITY STANDARDS

ROCK STEVENS, KEVIN HALLIDAY, MICHELLE MAZUREK // UNIVERSITY OF MARYLAND
JOSIAH DYKSTRA, JAMES CHAPMAN, ALEX FARMER // INDEPENDENT RESEARCHERS
WENDY KNOX EVERETTE // LEVIATHAN SECURITY GROUP
GARRETT BLADOW // DRAGOS, INC.

What are compliance standards?

Series of controls or policies that establish a baseline of security

Why use compliance standards?

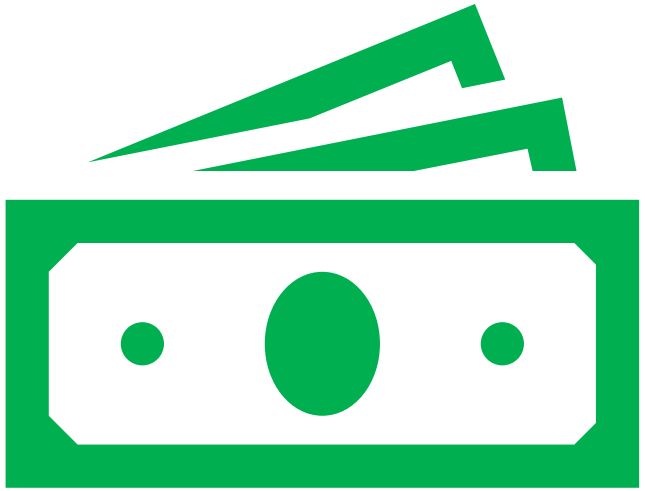
Mandatory to provide critical services or access to sensitive data

How is it enforced?

Audits

Financial sanctions

Privilege revocation



Vendor @ RSAC20 selling compliance

So what's the problem?

False sense of security

Never intended to be used as a checklist

Even if you had perfect compliance, what else could go wrong?

First empirical evaluation of compliance standards for security issues that exist **because of** perfect compliance

Audited Standards

Internal Revenue Services Publication 1075

Payment Card Industry Data Security Standard

North American Electric Reliability Corporation Critical Infrastructure Protection 007-6

Our methodology

Audit

External expert evaluation

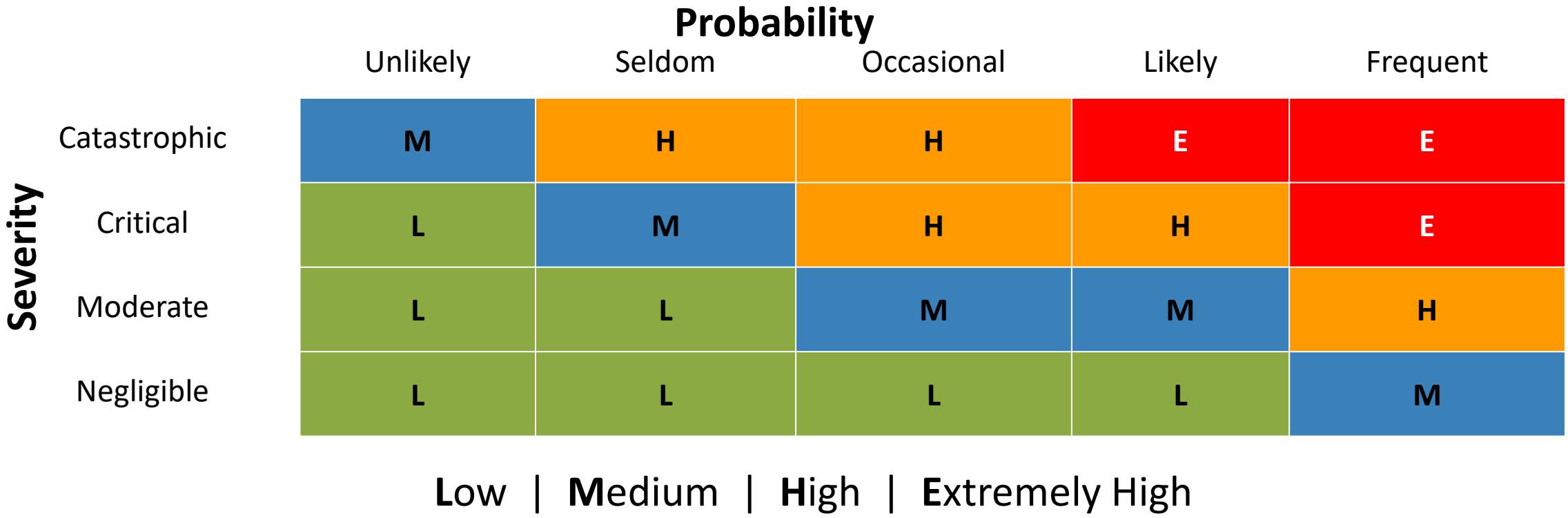
Disclose

Audit intent

Leverage real-world experience

Match to exploitation in the wild

Determine root cause



Determining risk estimates

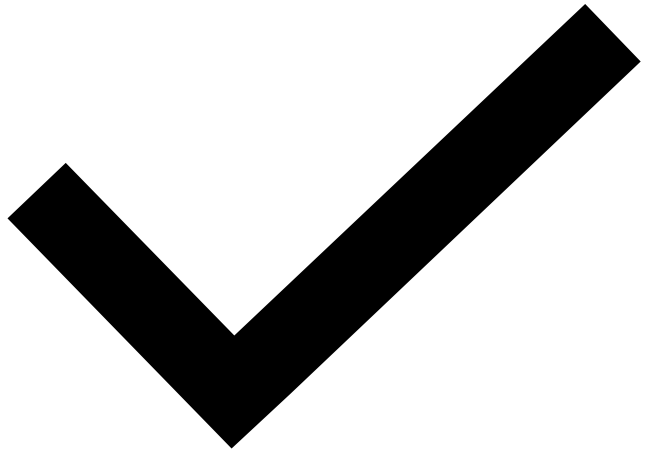
External expert evaluation

Recruited CISOs and compliance authors

Validate findings

Challenge our assumptions

Provide additional context



Disclose findings

Inform authors/councils

Inform users of standards

Exercise existing vuln disclosure processes

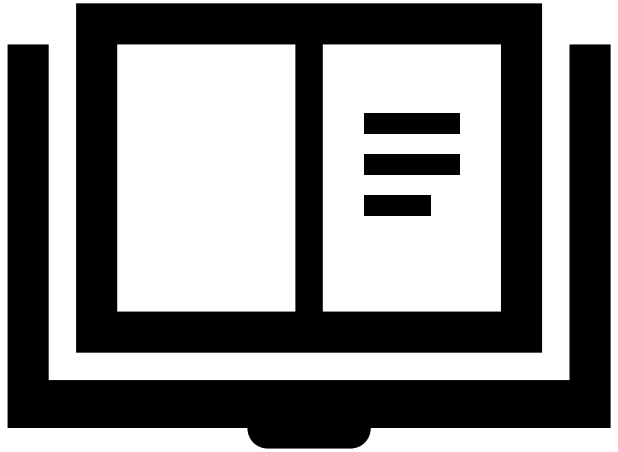
Results

Audit: By the numbers

3 standards

148 issues

4 root causes



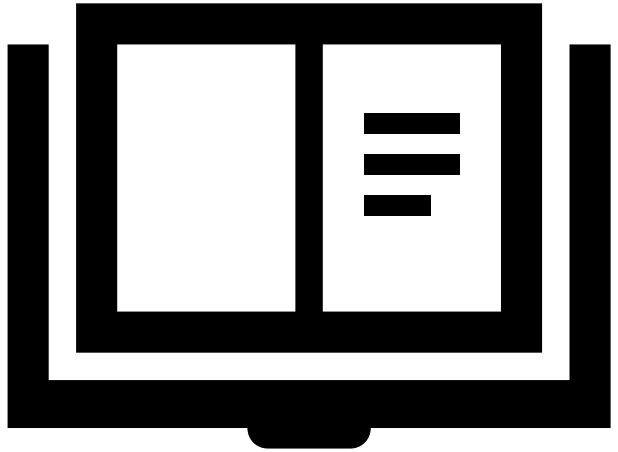
Audit: Root causes

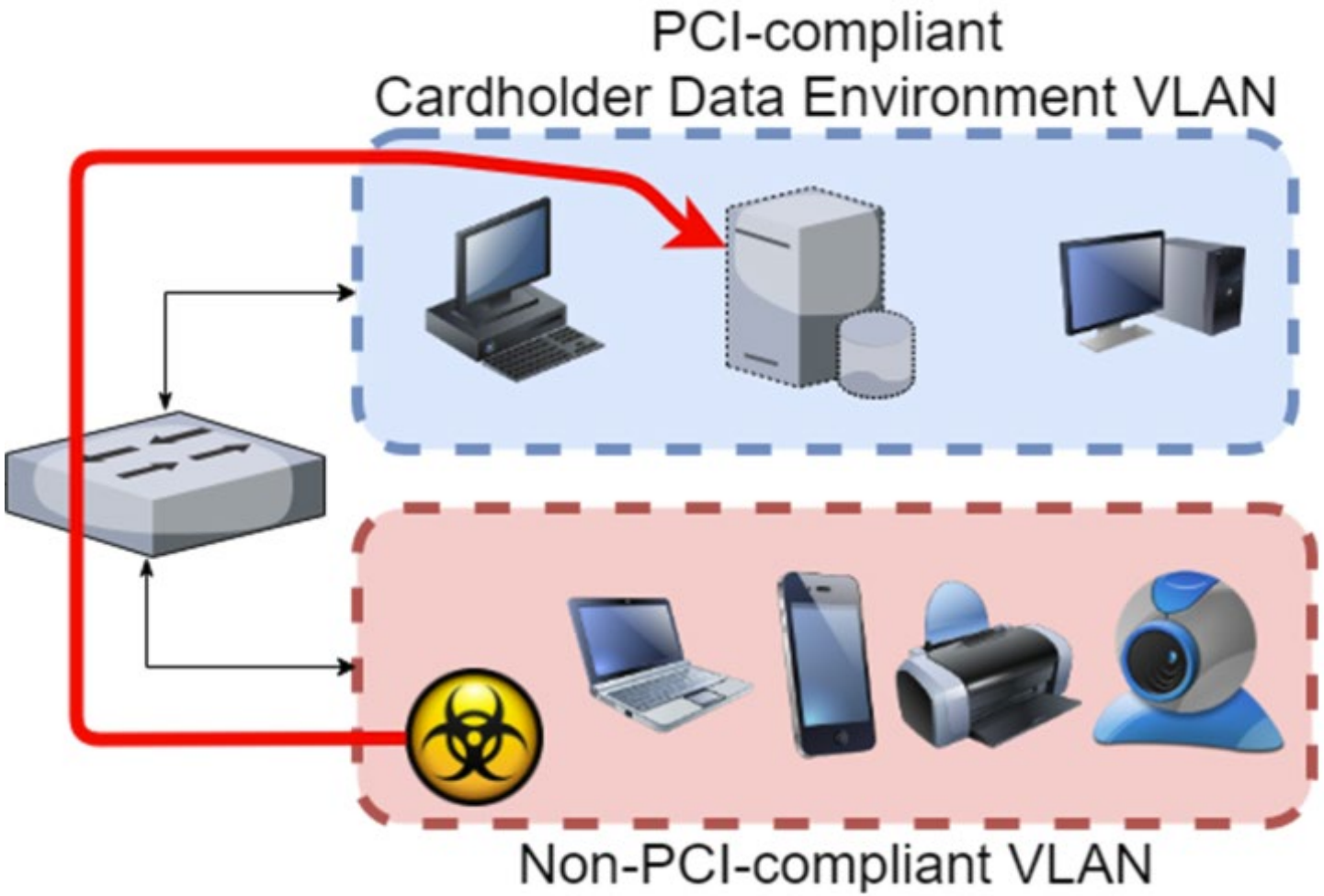
Data vulnerability

Unenforceable

Under-defined process

Ambiguous specification



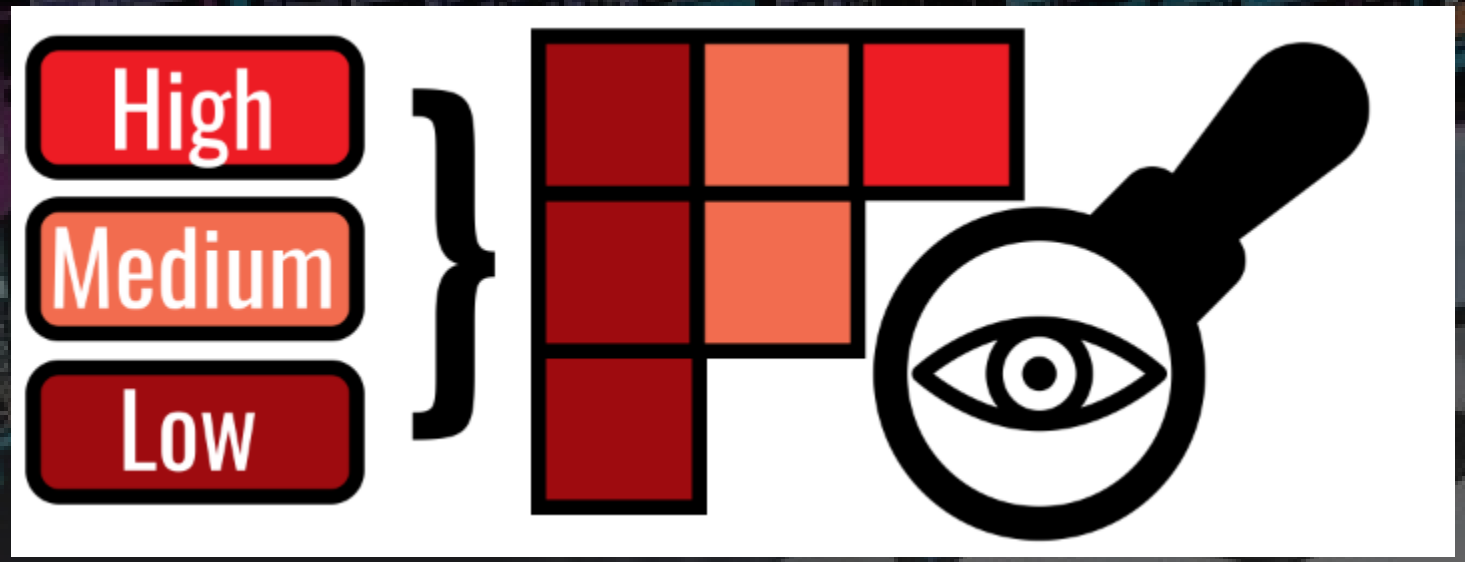


Data vulnerability

PCI DSS only protects enclave with cardholder data

Data vulnerability

Electric grid standards allows for variable security based on power production levels



Unenforceable

IRS P1075 requires multiple forms of physical security to protect data

and

Authorizes telework/remote access to data

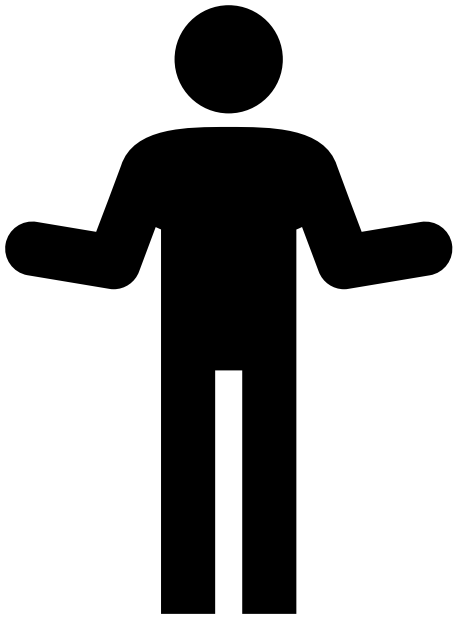
Under-defined process

IRS P1075 mandates a network component inventory

but

Never establishes “ground truth”

Ambiguous specification



IRS P1075: access control policies to be evaluated every 3 years.

By whom?

PCI DSS: all issues identified during a pentest must be addressed.

By when? Priority?

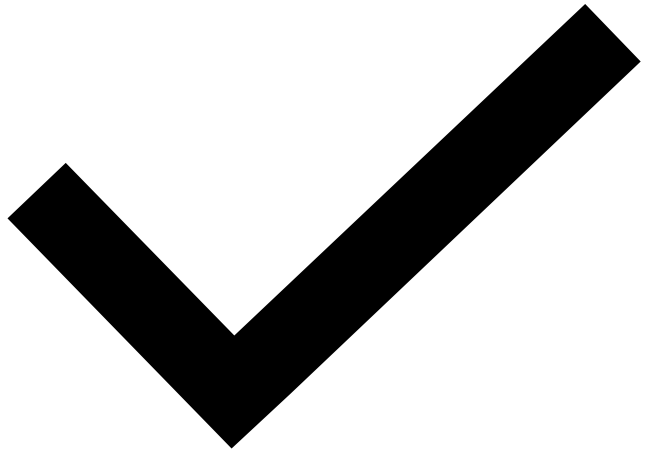
External expert evaluation

“Checklist compliance” confirmed

36/49 issues confirmed

10 plausible

3 rejected (kinda)



Disclosure attempts

US-CERT

National Vulnerability Database

MITRE Corp

“Each issue that requires a separate patch can get a CVE”

Disclosure attempts

NIST discussions on checklists

DHS “cease communications”

Disclosure attempts

PCI Council made updates based on findings

IRS ignored all calls/texts/emails

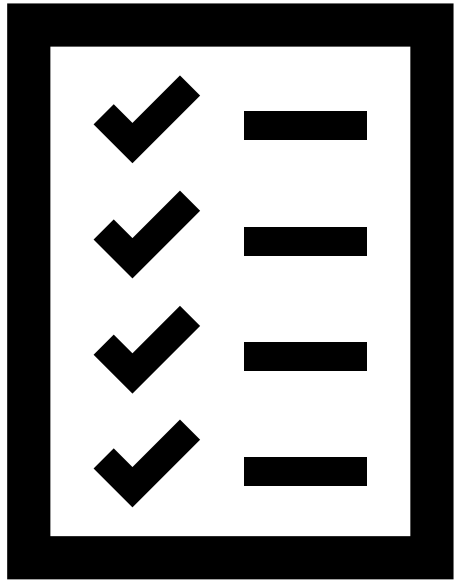
Recommendations

Make checklists

Solidify language to eliminate ambiguity

Orgs should conduct self-assessments

Better disclosure process



Summary

Perfect compliance != perfect security

- Ambiguous specifications and under-defined processes
- Lack of reporting makes fixing known problems harder

First study to empirically identify issues associated with compliance

Developed methodology for assessing other frameworks

> Questions / Feedback? rstevens@cs.umd.edu | @ada95ftw