



LASER Workshop 2020

Compliance Cautions

Investigating Security Issues Associated with
U.S. Digital-Security Standards

Rock Stevens, Kevin Halliday, Michelle Mazurek
Josiah Dykstra, James Chapman, Alexander Farmer
Wendy Knox Everett
Garrett Bladow

// University of Maryland
// Independent Researchers
// Leviathan Security Group
// Dragos, Inc.

Compliance Standards

- ◀ What are they?
- ◀ Why use them?
- ◀ How are they enforced?
- ◀ What's the problem?



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

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



Standards we examined



Study Methods

1

Audit

Six researchers conducting line-by-line audit of three standards

2

Expert evaluations

Four compliance experts evaluate researchers' findings

3

Disclosure

Various approaches to responsibly disclose findings to organizations

1

Audit

Six researchers conducting
line-by-line audit of three
standards

Real-world experience
Exploitation in the wild
Unanimous agreement

		Probability				
		Unlikely	Seldom	Occasional	Likely	Frequent
Severity	Catastrophic	M	H	H	E	E
	Critical	L	M	H	H	E
	Moderate	L	L	M	M	H
	Negligible	L	L	L	L	M
		E - Extremely High		H - High		M - Moderate
						L - Low



1

Audit

Six researchers conducting
line-by-line audit of three
standards

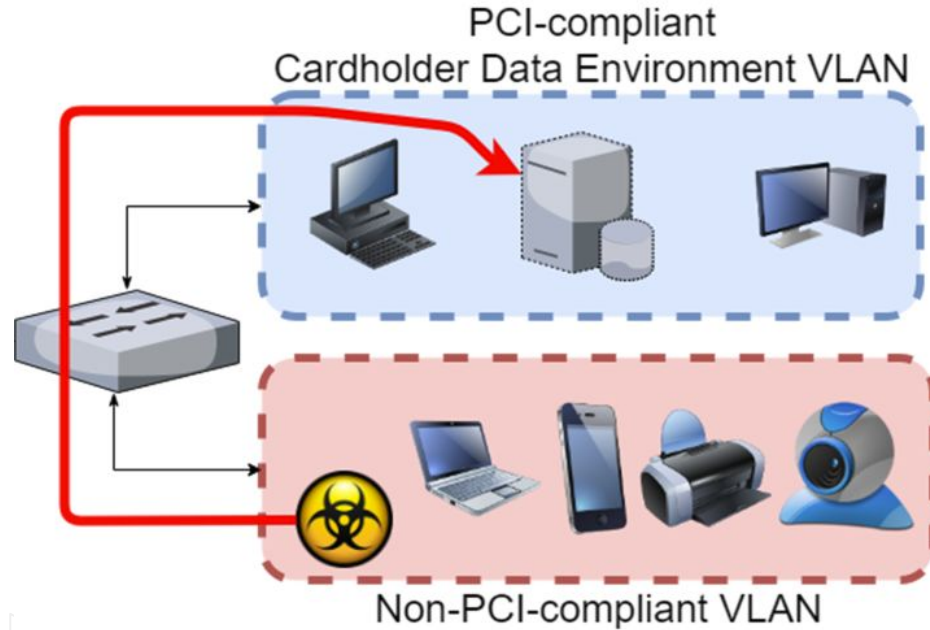
In total, **148 issues** ranging
from low to **extremely high**
risk

1

Audit

Six researchers conducting line-by-line audit of three standards

Data vulnerability

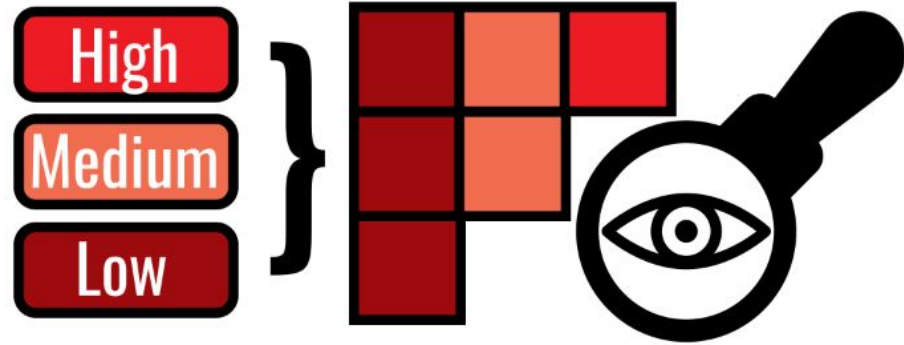


Data vulnerability

1

Audit

Six researchers conducting line-by-line audit of three standards

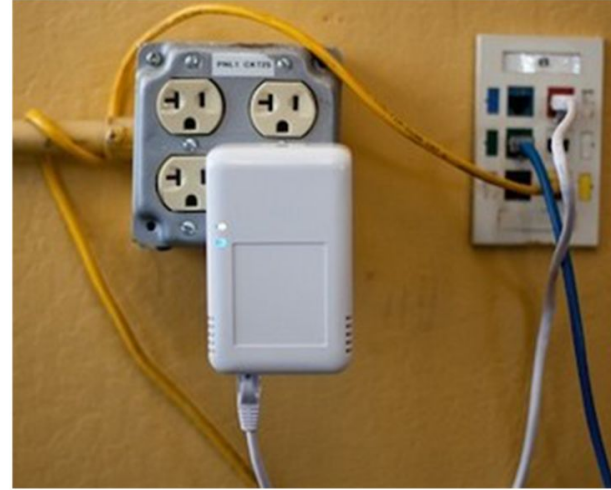


Under-defined process

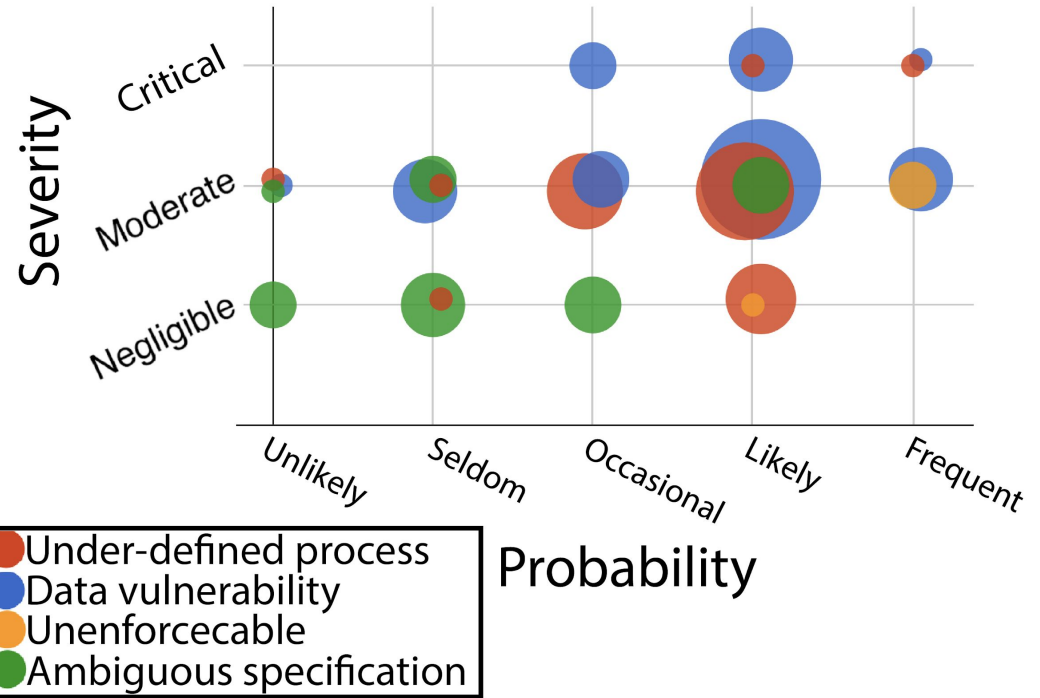
1

Audit

Six researchers conducting
line-by-line audit of three
standards



Risk Estimates for IRS Compliance Standard



LASER Talking Points, Pt 1

- Cold calling the experts!
 - **Friends/past contacts**
 - **Industry experts met at previous conferences**
- Interrater reliability
- Codebook development

LASER Talking Points

- Interrater reliability
 - **How to get results when people are in 4 different time zones, and everyone has a full-time job??**
 - **Calculated with Krippendorff's alpha**
- Codebook development

ID	Employment ¹	Role ²	Org Size	IT Exp (yrs)	Edu ³	Docs ⁴
R1	A, G	M, R	500	18	MS	I,P,N
R2	G	M, R	10k+	16	PhD	I,P
R3	A, G*, I	M, R	100	20	BS	I,N
R4	I	M, R	35	15	JD	I,P
R5	A, G*, I	M, D	100	8	BS	I,N
R6	G	M, D	100	5	BS	I,N
E1	G, I	M	150	10	BS	I
E2	G	M	150	15	MS	I
E3	G*, I	M, D	1k	18	MS	P
E4	A, G*, I	R	5k	20	MS	N

¹ A: Academia, G: Government, I: Industry, *: Previous experience

² M: Management, R: Research, D: Development

³ BS: Bachelor's, MS: Master's, PhD: Doctorate, JD: Juris Doctorate

⁴ I: IRS P1075, P: PCI DSS, N: NERC CIP

LASER Talking Points

ID	Employment ¹	Role ²	Org Size	IT Exp (yrs)	Edu ³	Docs ⁴
R1	A, G	M, R	500	18	MS	I,P,N
R2	G	M, R	10k+	16	PhD	I,P
R3	A, G*, I	M, R	100	20	BS	I,N
R4	I	M, R	35	15	JD	I,P
R5	A, G*, I	M, D	100	8	BS	I,N
R6	G	M, D	100	5	BS	I,N
E1	G, I	M	150	10	BS	I
E2	G	M	150	15	MS	I
E3	G*, I	M, D	1k	18	MS	P
E4	A, G*, I	R	5k	20	MS	N

¹ A: Academia, G: Government, I: Industry, *: Previous experience

² M: Management, R: Research, D: Development

³ BS: Bachelor's, MS: Master's, PhD: Doctorate, JD: Juris Doctorate

⁴ I: IRS P1075, P: PCI DSS, N: NERC CIP



LASER Talking Points

- Codebook development
 - **Determine root cause**
 - **Do it iteratively until you have agreement**
 - **Define terms upfront!!!**

2

Expert evaluations

Four compliance experts evaluate researchers' findings

CISOs and authors
Challenge assumptions
Validate findings
Provide context

LASER Talking Points, Pt 2

2

Expert evaluations

Four compliance experts evaluate researchers' findings

**Confirmed
real-world misuse of
compliance
standards**

▶ **“White box” pentest**

3

Disclosure

Various approaches to responsibly disclose findings to organizations

Enforcers
Creators
Aggregators

3

Disclosure

Various approaches to responsibly disclose findings to organizations

RFCs closed

RFCs

CVEs

"Not my Job"

NDA's

Direct reporting

Centralized repository

Federal reporting

Cease communications!

What did you try that did not succeed before getting to the results you presented?

8 months to finish first part,
8 months of NDA negotiations, and
Several follow-on interviews to clarify survey data

Wrap-up

- Wrap up discussion
- Next steps?
- Plans for post-workshop paper?

> **Questions / Feedback?** rstevens@cs.umd.edu | [@ada95ftw](https://twitter.com/ada95ftw)