A Practitioner's View of the Ohio Data Protection Act

Presented to the 2019 Central Ohio Infosec Summit

Justin Hall

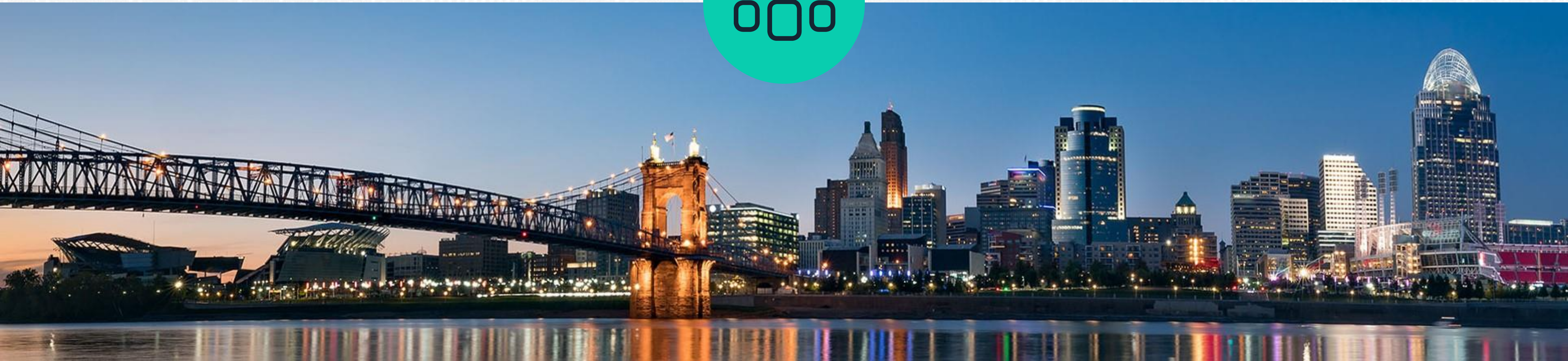
Director, Security Consulting

cbts

/usr/bin/whoami

- Cincinnati native
- Husband & dad
- 20+ years in IT
- 14+ years in security

- Director of Security Consulting at CBTS
- GCIH Gold / GCFA / GPEN
- University of Cincinnati College of Business alumnus



I am not a lawyer.

This presentation is not intended to be legal advice, but a general discussion about the Ohio Data Protection Act.

If you require legal advice, you are advised to consult a qualified lawyer in your jurisdiction.

All of this is speculation.

The Ohio Data Protection Act is brand spankin' new.

There is no existing case law involving this legislation.

I'm guessing on pretty much all of this (but it's an educated guess FWIW).

In the last decade…

TARGET

Date of breach: Nov 2013

Settlement: **$18.5 million**

Wendy's

Date of breach: July 2016

Settlement: **$50 million**

THE HOME DEPOT

Date of breach: April 2014

Settlement: **$27.5 million**

YAHOO!

Date of breach: 2013/2014

Settlement: **$85 million (possibly more)**

About the ODPA

cbts

About the Ohio Data Protection Act

Ohio SB220

Signed August 3, 2018

Effective November 2, 2018

Provides an **“affirmative defense”** from tort claims originating from a breach that involve personal information

Requires that covered entities “**create, maintain, and comply with** a written cybersecurity program”

Terms to understand: Affirmative Defense

cbts

"This is a defense in which the defendant introduces evidence, which, if found to be credible, will **negate criminal liability or civil liability**, even if it is proven that the defendant committed the alleged acts."

Cornell Legal Information Institute, *Affirmative Defense*, *available at https://www.law.cornell.edu/wex/affirmative_defense (last visited 4/8/2019)*

Terms to understand: Cybersecurity Program

A document 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”

The program described **must**:

“Protect the **security and confidentiality** of the information;

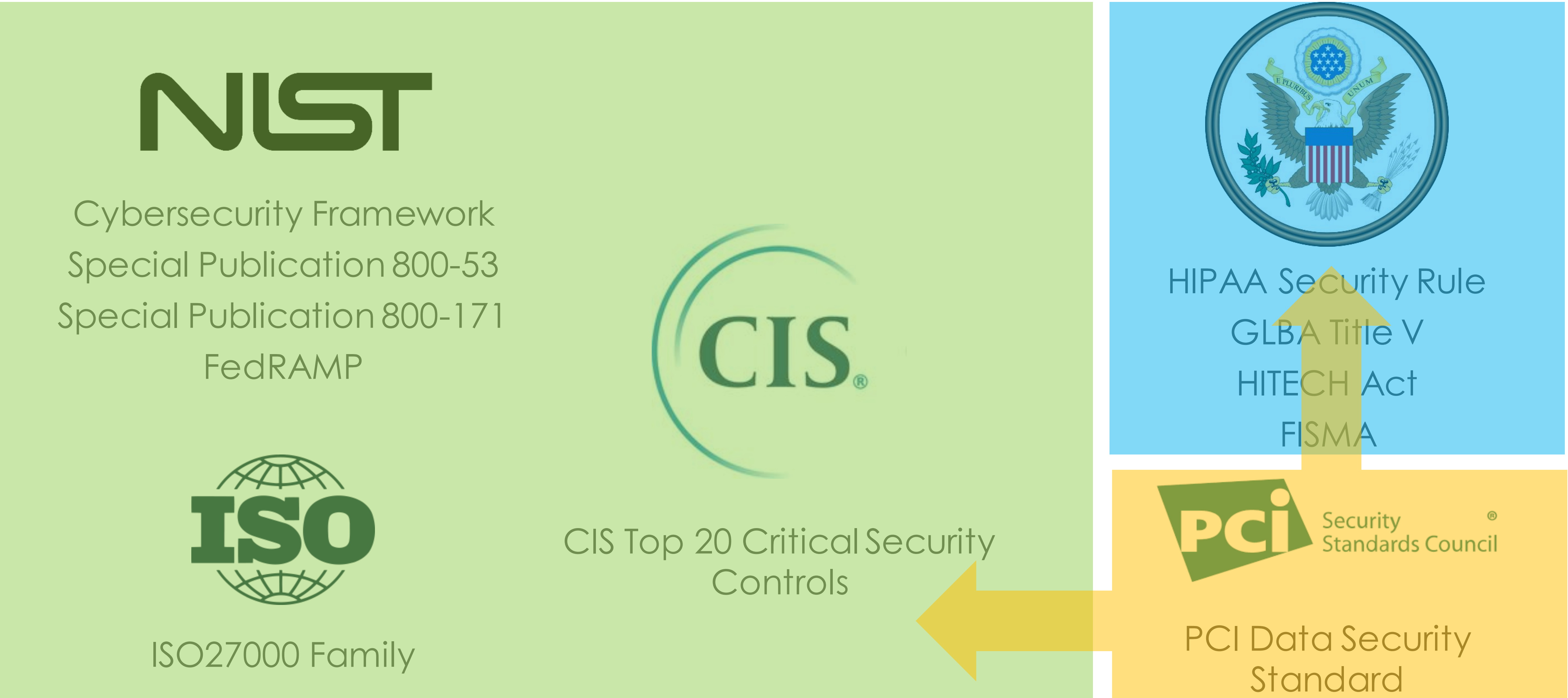
Protect against any **anticipated threats or hazards** to the security or integrity of the information;

Protect against **unauthorized access to and acquisition of the information** that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.”

Program Requirements

- The entity must **create**, **maintain**, and **comply** with the cybersecurity program
  - **Create** = *write it down*
  - **Maintain** = *keep it up to date*
  - **Comply with** = *do the thing you wrote down*
- The cybersecurity program must be designed to **protect information**
- The cybersecurity program must conform to an **approved framework**
- The cybersecurity program must be "**appropriate**" for the covered entity

Approved Security Frameworks



NIST

Cybersecurity Framework
Special Publication 800-53
Special Publication 800-171
FedRAMP

ISO

ISO27000 Family

CIS

CIS Top 20 Critical Security Controls

HIPAA Security Rule
GLBA Title V
HITECH Act
FISMA

PCI Security Standards Council

PCI Data Security Standard

Terms to understand: Appropriate Program

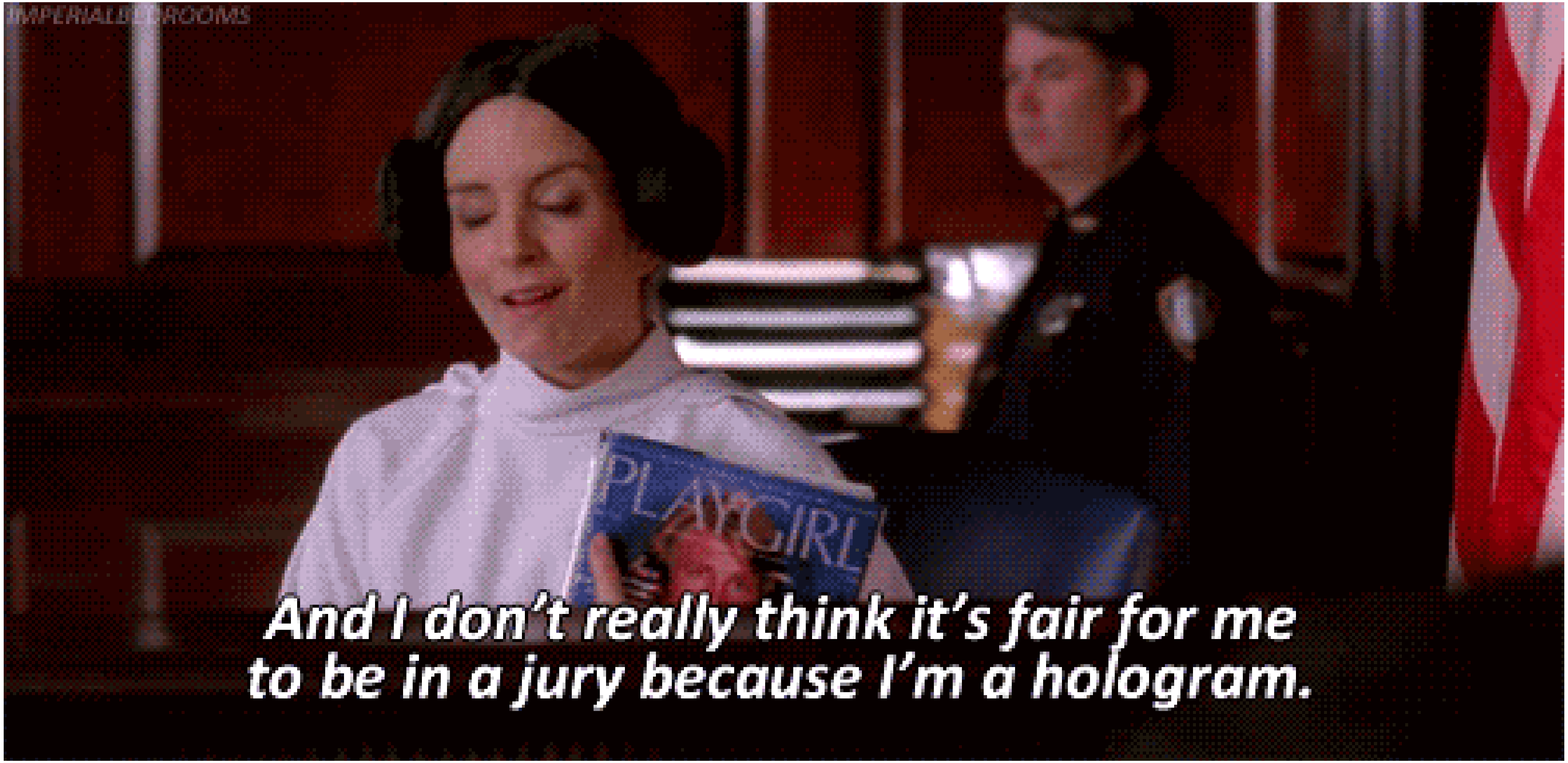
Five factors determine if your security program is appropriate for your organization:

1. The **size and complexity** of the covered entity
2. The **nature and scope of the activities** of the covered entity
3. The **sensitivity of the information** to be protected
4. The **cost and availability of tools** to improve information security and reduce vulnerabilities
5. The **resources available** to the covered entity

An Analysis of the Law and How To Prepare

To Summarize:

Convincing a Jury


IMPERIALBEDROOMS
And I don't really think it's fair for me
to be in a jury because I'm a hologram.

Building a Convincing Case

What kind of evidence is impactful?

#1 Policy

- Broad Information Security Policy
  - Mission and vision
  - Roles and responsibilities
  - Metrics
- Incident Response Policy
  - How Breaches Are Handled
  - Notification & Communication
- Data Protection/Classification Policy
- Acceptable Use Policy
- Application Security Policy
- Security Architecture/Infrastructure Design Requirements
- Endpoint Hardening Policy & Process
- Data Retention/Destruction Policies
- Security Monitoring & Logging Policy
- Third Party Vendor/Supplier Security & Risk Policy
- Physical Security Policy

Building a Convincing Case

What kind of evidence is impactful?

#2 Operational Playbooks

- Incident Response
  - Ongoing monitoring, triage, analysis (Identification phase)
  - Specific investigation use cases
  - Forensics & live response
  - Containment, Eradication, Recovery, Lessons Learned phases
- Security Architecture
  - Design, Build, Run phases
- Vulnerability Management
  - Bulletin collection, triage
  - Ongoing vulnerability assessment
  - Red team/purple team
  - Third party assessment
  - Patch management, testing, validation
- Software Development
  - SDLC & Security Reviews
  - DevSecOps

Building a Convincing Case

What kind of evidence is impactful?

cbts

#3 Security Metrics

- NIST Cybersecurity Framework
  - Company's current **Framework Profile** and **Framework Implementation Tier (Tier 1-4)** for each domain
- ISO27K Information Security Management System
  - 27001 has 18 domains
  - No inherent scoring/measurement system
  - **Carnegie Mellon CMM** helps
- Vulnerability Management
  - Patching metrics & vulnerability remediation
  - Results of third party assessments
- Security Monitoring & Response
  - **Mean Time To Detect & Mean Time To Remediate**
  - Size & scope of monitoring and response effort, staffing, toolset
- **Growth strategy for all areas!**

Q&A

Thanks!

cbts

cbts.com/security