ISO27001 Assessment

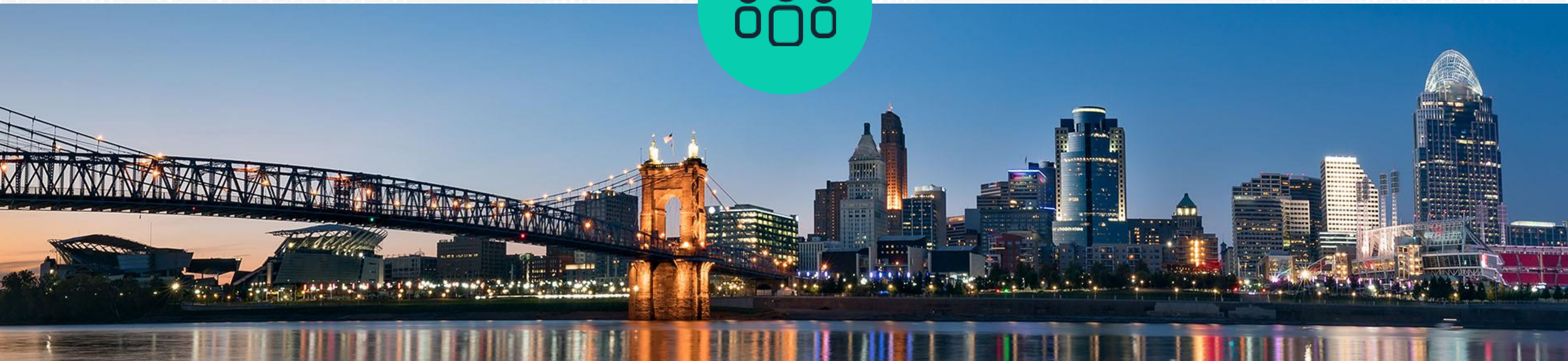
Mitsubishi Electric Americas
IT Managers Meeting
Spring Security Conference 2019

Justin Hall
Director, Security Consulting

cbts

/usr/bin/whoami

- Born & raised in Cincinnati
- 23 years in IT
- 14 in Infosec
- BBA, Information Systems – University of Cincinnati
- GCIH Gold, GCFA, GPEN
- Cofounded Cincinnati Infragard DFWG, Bsides Cincinnati, Cincy Security Exchange
- Director, Security Consulting at CBTS

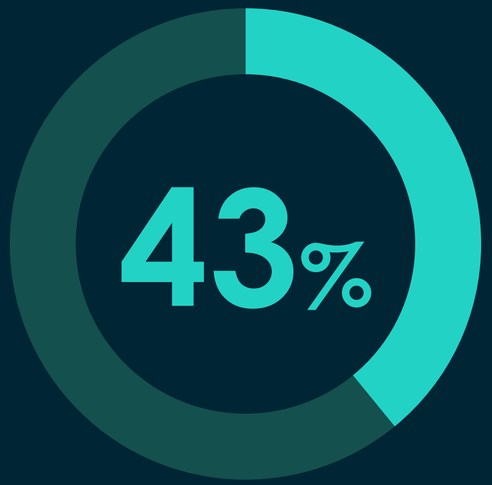


Agenda

- Current threat landscape
- Where ISO fits
- Measuring program progress
- About the Carnegie Mellon CMMI
- Setting maturity development goals
- Internal vs third party assessment
- Technical control capability
- Q&A

2246

Companies in the United States reported a data breach in 2018.



of reported breaches were from three industries:

- Financial & Insurance
- Healthcare
- Government & Public Administration

Source: Risk Based Security 2018 Report

1 in 412

Email messages are malicious

1 in 10

URLs accessed by clients are malicious

5200

IoT / Smart devices experience 5200 attacks per month

New in 2018

246M Malware variants

187M Ransomware variants

2300 Mobile malware variants

Regulatory Compliance

Confusing Product Landscape

New Threats and Vulnerabilities

Skills and Resources Gap

The ISO27001-Based Security Program

The ISO Model For Building A Security Program

Requirements → Scope → Information Security Management System → Objectives

Objectives

Actions

Risk Assessment

Risk Treatment

Effectiveness Measurement

Measuring The Program

Monitoring
Measurement
Analysis Evaluation

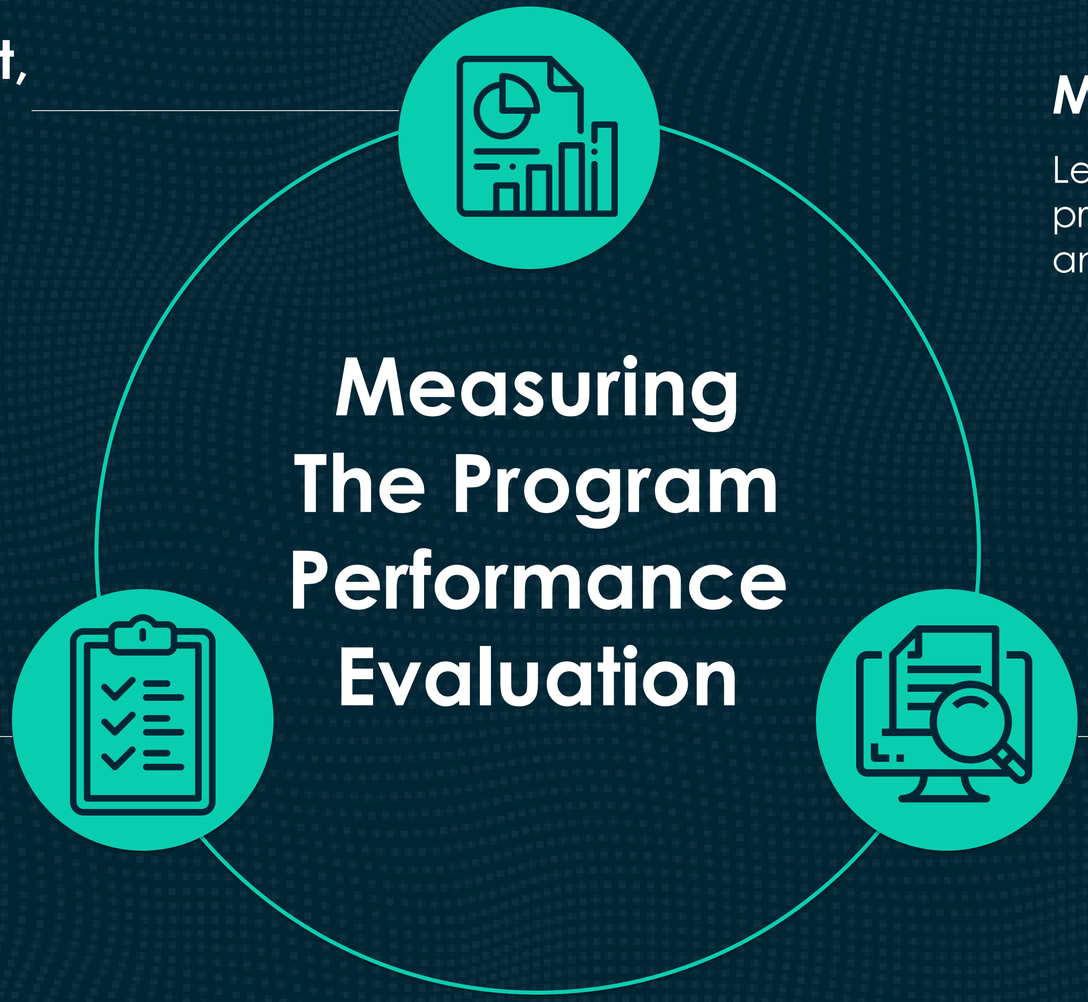
Internal Audit

Management Review

Nonconformity &
Corrective Action

Continuous
Improvement

Measuring The Program Performance Evaluation



Monitoring, Measurement, Analysis, Evaluation

Self-developed metrics act as guard rails that ensure team produces valid results

Management Review

Leadership perspective provides business context and overall risk view

Internal Audit

Separate team that objectively assesses program's capabilities and effectiveness

The Carnegie Mellon Capability Maturity Model Integration

"The Capability Maturity Model Integration (CMMI)® is a proven set of global best practices that **drives business performance** through building and benchmarking **key capabilities.**"

Translation:

A **process improvement framework** that helps **measure** the maturity of, and **plan growth** for, a variety of business operations.

Applying CMMI To ISO27000

Security Maturity Levels >	0: Nonexistent	1: Initial	2: Repeatable	3: Defined	4: Managed	5: Optimized
Maturity Level Description >	There is no evidence of this standard or practice in the organization.	The organization has an ad hoc and inconsistent approach to this privacy standard or practice.	The organization has a consistent overall approach, but it is mostly undocumented.	The organization has a documented, detailed approach, but no routine measurement or enforcement of it.	The organization regularly measures its compliance and makes regular process improvements	The organization has refined its compliance to the level of best practice.
Process consistency	None	Ad hoc	Consistent	Consistent	Consistent	Consistent
Process documentation	None	None	Minimal, high-level	Detailed	Detailed	Detailed
Business objectives	None	Not Met	Partially met	Mostly met	Fully met	Value added
Process measurement	None	None	None	Ad hoc	Routine	Systemic
Policy enforcement	None	None	None	Ad hoc	Routine	Systemic
Process improvement	None	Ad hoc	Ad hoc	Ad hoc	Routine	Systemic
Process benchmarking	None	None	None	Ad hoc	Ad hoc	Routine
Corresponding Level of Risk of a Data Breach or Regulatory Noncompliance	**Very high** across the organization	**High** across the organization, and **very high** in key parts of the organization	**Moderate** across the organization, with some pockets of **high** risk.	**Moderate** across the organization.	**Low** across the organization.	**Remote** across the organization.

Domain	Maturity Rating
Information Security Policies	3
Organization of Information Security	3
Human Resource Security	1
Asset Management	4
Access Control	2
Cryptography	3
Physical and Environmental Security	2
Operations Security	2
Communications Security	2
Systems Acquisition, Development and Maintenance	2
Supplier Relationships	1
Information Security Incident Management	3
Information Security Aspects of Business Continuity Management	1
Compliance	2
Average	2

Setting Goals For Growth

1. Choose a functional area
2. Aim for a single tier of improvement
3. Determine which controls would effect this improvement
4. Establish projects to implement controls
5. Aim for 2-3 functional areas to target per year

Setting Goals For Growth

“Process Consistency”	**1: Initial 2: Repeatable**	**Patch Management**	**Goal: Update 95% of assets within 30 days of patch release**	
1	2	3	4	5
Choose a functional area	Aim for a single tier of improvement	Determine which controls would effect this improvement	Establish projects to implement controls	Aim for 2-3 functional areas to target per year

When To Bring In A Third Party To Assess?

Regulatory requirements demand it

Growth has **ceased**

Resource **limitations**

New staff needs new direction

Technical Control Guidance Options

NIST 800-53r5

A catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks.

CIS Critical Security Controls

A prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

How to Engage Us

Justin Hall - Director, Security Consulting
justin.hall@cbts.com | 513.252.6011

Tim Linder - Director, Security Sales
tim.linder@cbts.com | 513.706.5270

Questions?