Cybertrack Report:
Aggregate Results & Analysis from the first Twenty-Three Assessments

Indiana's Local Government Cybersecurity Assessment Program

November 2023

Joe Beckman, Purdue University cyberTAP
Craig Jackson, Indiana University Center for Applied Cybersecurity Research
Emily K. Adams, Indiana University Center for Applied Cybersecurity Research
Ranson Ricks, Indiana University Center for Applied Cybersecurity Research
Leigh Ann Griffin, Purdue University cyberTAP
Kelli Shute, Indiana University Center for Applied Cybersecurity Research
Scott Russell, Indiana University Center for Applied Cybersecurity Research
Phil Conrad, Purdue University cyberTAP
Mark Krenz, Indiana University Center for Applied Cybersecurity Research

Table of Contents

About Cybertrack

With sponsorship from the Indiana Office of Technology (IOT), Purdue University and Indiana University have partnered to develop Cybertrack: Indiana's local government cybersecurity assessment program. Cybertrack is designed to put local governments in contact with top tier cybersecurity experts and provide them **practical, prioritized advice about doable, powerful cybersecurity fundamentals.** Our goal is to make Indiana more secure in the short term and shape our collective cybersecurity strategy and policy for the long term. Cybertrack cybersecurity assessments are available for no fee to Indiana local government entities.

The primary deliverable of each assessment is a report which includes evaluations of organizational cybersecurity fundamentals and safeguards, actionable recommendations, and explanations thereof. The recommendations emphasize individual local government's cybersecurity strategies, with a particular focus on short-term priorities.

Purdue University and Indiana University are two of the nation's leading universities in cybersecurity, with complementary technical and programmatic strengths as well as common commitments to practical cybersecurity and the value of cybersecurity assessments.

For additional information about Cybertrack, visit the program's website: https://incybertrack.org or contact: Joe Beckman, beckmanj@purdue.edu or Craig Jackson, scjackso@iu.edu.

Acknowledgements

The Cybertrack Team thanks the Indiana local governments that assisted the development of our assessment process by serving as pilot organizations.

Cybertrack is supported by funding from the Indiana Office of Technology (IOT). The views expressed in this report do not necessarily reflect the views of the IOT or any other organization.

1 Executive Summary

This is the first report of aggregate assessment results and analysis from Cybertrack: Indiana's Local Government Cybersecurity Assessment Program. The program serves a diverse set of Indiana's local entities, including counties, cities, and towns. This report covers aggregated results from Cybertrack's first 23 of the planned 342 assessments. The Cybertrack Program is ongoing, with new assessments starting and ongoing ones completing every month. As such, these are early results and our ability to draw strong conclusions about correlations and patterns around the Hoosier State are somewhat limited. At the same time, these early results offer some initial and potentially guiding insights into the current state of cybersecurity for Indiana's local government entities.

One of Cybertrack's primary goals is to inform Indiana's local government cybersecurity policy and strategy. This report supports that goal. This analysis is an initial contribution to shaping our collective cybersecurity strategy and policy for the long term. We've written this report with a wide-ranging audience in mind, including state and local policymakers. **Considering Cybertrack only assesses a subset of cybersecurity practices that are known to be among the most powerful, the early results are sobering.** (*See* **Figures 1 and 2**, on the following pages.) **Indiana's local government entities have a long way to go on basic cybersecurity capability, and they most certainly need help.**

Key Takeaways. Early results include the following trends.

- **Senior organizational leadership is involved in cybersecurity decision making in about half of assessed organizations.** In our Trusted CI Framework-based assessment of organizational, programmatic cybersecurity fundamentals, this was a relatively positive result, but clearly more leadership attention is needed across the community. **We saw more concerning results when it came to basic formalization of cybersecurity governance, policy, budgets, and personnel resource allocation**. **Indiana local government entities should prioritize these organizational fundamentals. They are necessary to support sound decision making and cybersecurity investment.**
- At the more technical, tactical level, most Indiana local government entities are struggling to implement even the most fundamental, powerful controls. Results from "Inventory and Control of Software Assets" (CIS Control 2) Safeguards are a particularly extreme example of these struggles with no assessed entities implementing them. **Even the most empirically-proven controls among those we assessed, *e.g.*, multi-factor authentication (MFA) and secure configuration, showed concerningly low rates of implementation.** For example, MFA has been implemented on remote access applications in 30% of assessed entities. MFA for administrative access has been implemented in only 13% of assessed entities. **The community should prioritize all the Safeguards covered in this assessment, with particular attention to the most proven: These include the Transformative Twelve (see Figure 2 and Section 2.1).**

We also see reason for optimism: We've heard strong positive feedback on the assessment experience including the highly prioritized nature of our recommendations, and strong interest in finding ways to progress not only as individual organizations, but also as a community.

Roadmap for the report. Section 2 (Methodology) describes the Cybertrack assessment methodology, including what we assess, why we assess it, and how we assess it, as well as how we aggregated and analyzed the data from those assessments. Section 3 (Results) provides an overview of the aggregated assessment results to date. Section 4 (Analysis) analyzes those early results, highlighting noteworthy patterns and themes. Finally, Section 5 (Conclusion) offers perspectives on our early results and future directions of the Cybertrack program.

Figure 1. Distribution of Implementation Ratings for the First Twenty-Three Cybertrack Assessments

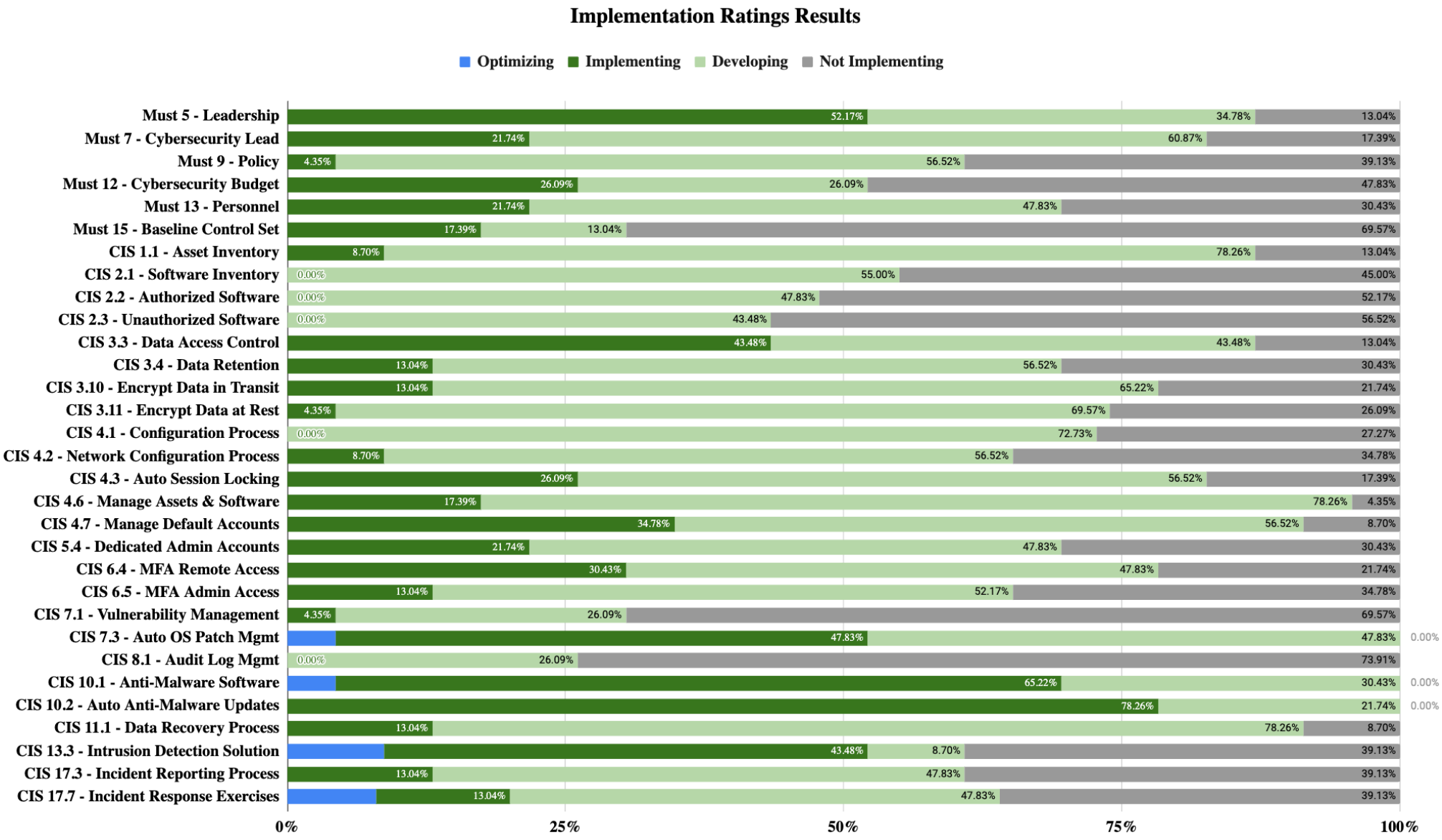
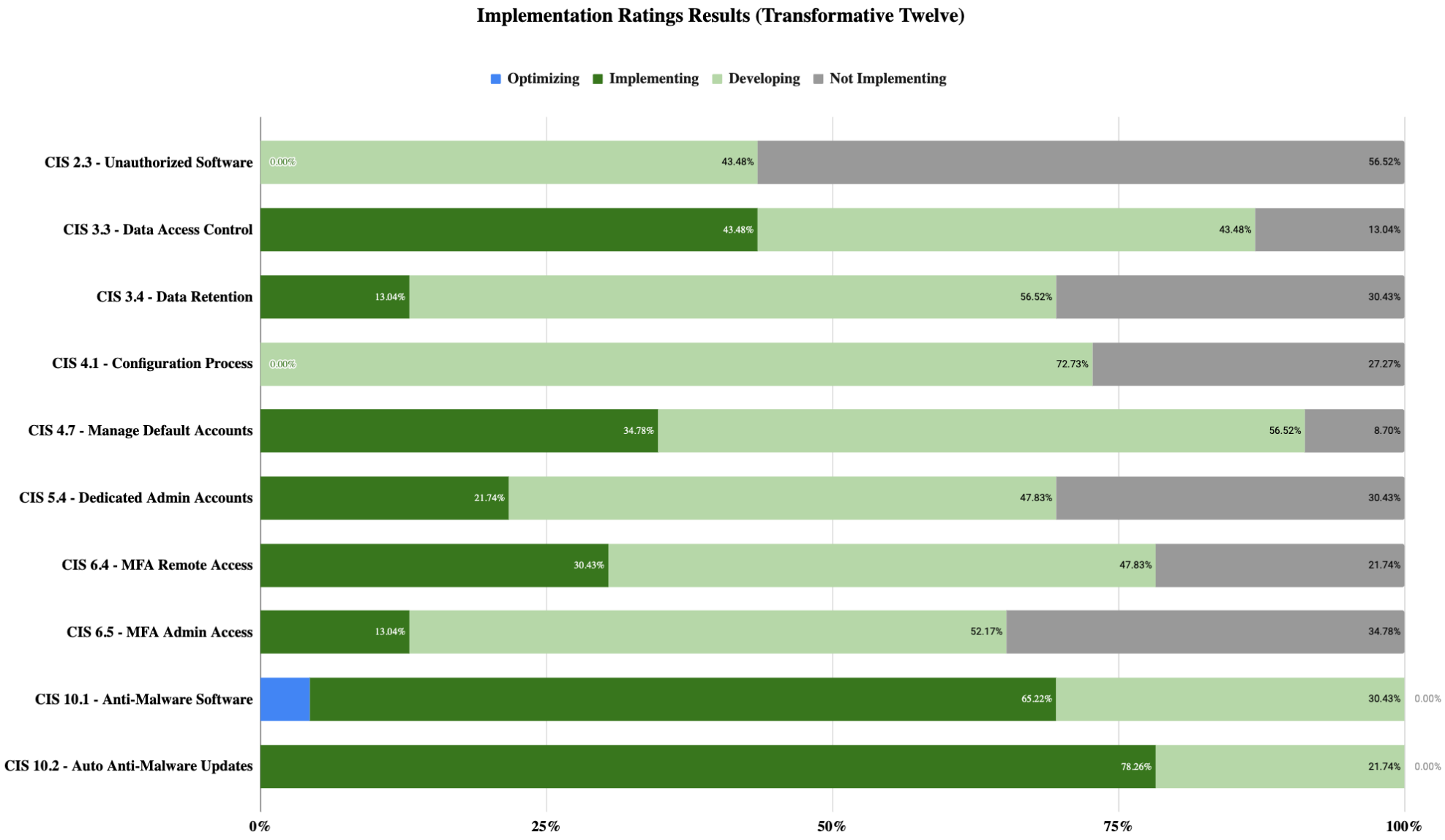


Figure 2. Distribution of Implementation Ratings for the First Twenty-Three Cybertrack Assessments (Transformative Twelve)



Two of the twelve were recently added after re-analysis: CIS 6.3: Require MFA for Externally-Exposed Applications and CIS 11.4: Establish and Maintain an Isolated Instance of Recovery Data. We will begin covering their results and trends in future reports.

2 Methodology

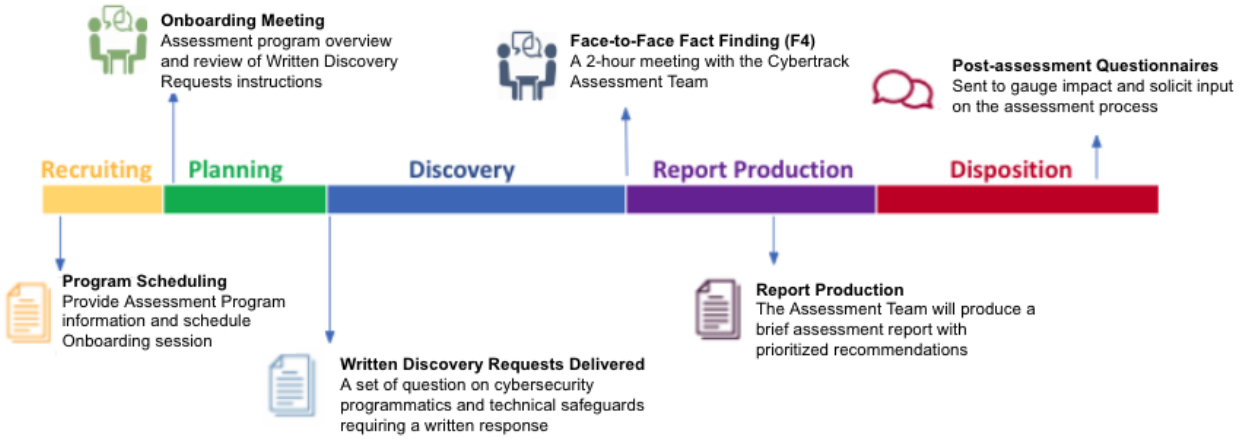
This section describes the Cybertrack assessment methodology, including what we assess, why and how we assess it, and how we aggregated and analyzed the data from those assessments.

2.1 Assessment Methodology

We built the Cybertrack assessment methodology by leveraging the Indiana University Center for Applied Cybersecurity Research's (IU CACR) expertise in cybersecurity assessment methodology development as well as Purdue's experience conducting CSET-based[1] assessments of local government entities. The assessment approach draws heavily from the US Navy's PACT cybersecurity assessment methodology,[2] and both institutions' extensive experience conducting assessments. The methodology is designed to be standardized, highly efficient, and effective at both helping local government entities prioritize the most doable, impactful actions, as well as building an overarching picture of the state of cybersecurity across the state.

Assessment Process. Each Cybertrack Assessment follows a standardized process (Figure 3). After expressing interest, representatives of local government entities attend an Onboarding Meeting where Cybertrack Team members explain the assessment process and where local government personnel can ask questions. After the Onboarding Meeting, the local government identifies the local government personnel who will be directly involved in the assessment (the "LG-Team"), and the Cybertrack Team delivers our standardized Written Discovery Requests (WDRs). These WDRs call for written responses, and are focused on a subset of the Trusted CI Framework Musts and CIS Safeguards discussed later in this section, as well as basic data characterizing the local government entity (*e.g.*, type, population, number of endpoints).

Figure 3. Cybertrack Assessment Phases



[1] CSET is software developed by the United States Department of Homeland Security, Cybersecurity & Infrastructure Security Agency to facilitate organizational cybersecurity assessments. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr.

[2] This methodology was developed by IU personnel (including Jackson), is based heavily on more than dozen prior assessments for the NSF Cybersecurity Center of Excellence and the US Navy, and has been successfully used in a wide range of environments. For more about PACT, *see* https://cacr.iu.edu/pact/index.html.

Each Cybertrack assessment leverages a two-person Assessment Team (one member from IU CACR, one member from Purdue cyberTAP), with a total effort allocation of 30 hours per assessment. After the LG-Team completes and returns responses to the WDRs, the Assessment Team completes an initial analysis followed by a Face-to-Face Fact Finding (F4) meeting with the LG-Team (and any other local government invitees). The F4 is a 2-hour meeting designed to clarify relevant facts and help the Assessment Team identify and tailor the recommendations that appear in the Assessment Report.

Each assessment report includes implementation ratings (*see* Section 2.2) for each Must and Safeguard we assess, and a small number of well-supported, highly-actionable recommendations. Each recommendation has Facts, Recommendation Detail, and Rationale sections. The recommendations emphasize individual local government's cybersecurity strategies, with a particular focus on short-term priorities.

After the report is delivered and time is allowed for the local government to review and consider the report, the Cybertrack Team follows up with post-assessment questionnaires to gauge impact and solicit input that can improve the assessment process.

Assessment Scope and Standards. The Cybertrack assessment's scope and focus is on the local government's organizational cybersecurity governance and resourcing, as well as security controls supporting its information, information technology, and operational technology[3].

This assessment is **focused on the most proven, most impactful, most fundamental organizational (aka "programmatic") "Musts" and "Safeguards."** The programmatic Musts were selected from the Trusted CI Framework.[4] The Safeguards were identified via research and alignment to federal grant programs, mapped to, and ultimately selected primarily from Implementation Group 1 of the CIS Controls v8.[5] The Musts and Safeguards covered in this assessment are listed in **Appendix A**.

The **Trusted CI Framework** is a minimum standard for cybersecurity programs, developed by IU CACR personnel for Trusted CI, the NSF Cybersecurity Center of Excellence. The Trusted CI Framework matches the goals for Cybertrack assessments because, unlike other cybersecurity frameworks, the Trusted CI Framework is focused entirely on organizational cybersecurity fundamentals, aka "programmatics." It consists of 16 "Musts," organized under four pillars: Mission Alignment, Governance, Resources, and Controls. **Each Must represents a foundational requirement for a competent cybersecurity program**. We selected 6 of the most basic Musts for inclusion in this assessment (*e.g.*, assessing whether leadership is involved in cybersecurity decision making; whether the organization has a cybersecurity lead role; whether the organization has a cybersecurity budget).

The **CIS Controls** "are a relatively short list of high-priority, highly effective defensive actions that

[3] Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. *See* https://csrc.nist.gov/glossary/term/operational_technology.
[4] https://www.trustedci.org/framework.
[5] https://www.cisecurity.org/controls.

provide a 'must-do, do-first' starting point for every enterprise seeking to improve their cyber defense."[6] They are 1) highly prioritized; 2) updated frequently; 3) described in sufficient detail for organizations to implement them; and 4) developed by a collaborative and open process informed by a diverse group of cybersecurity practitioners. They are applicable to a very broad range of organizations, including local government entities. They map readily to the controls in many other cybersecurity standards (*e.g.*, NIST CSF, NIST 800-53, SOC 2). Each Control is broken down into "Safeguards" that describe specific actions that organizations should take to implement the Control. Implementation Group 1 (IG1)[7] is a set of 56 Safeguards that "represents a minimum standard of information security for all enterprises"[8] and helps all organizations deal with the most common types of attacks we see in real life.

With efficiency and impact in mind, in order to downselect further the IU Team conducted research to identify an evidence-based, even more-highly prioritized subset of CIS Safeguards. We set out to identify "gold standard" systematic studies whose results point to a small set of proven high-power controls. To meet this "gold standard" we had to develop confidence in the validity of the methodology used in each candidate source. As such, we considered and eliminated a number of sources that lacked any publicly available documentation of their methodology. We found three studies that qualified: (a) the CIS Community Defense Model v2.0[9]; (b) the Microsoft Digital Defense Report[10]; and (c) the Australian Signals Directorate's Essential Eight.[11] Notably, each of these three studies used a different methodology. We mapped the identified controls to the appropriate CIS Safeguards and scored them: Safeguards received a score for each appearance in a gold standard study. Thus those Safeguards that appear in more gold standard studies received a higher score.

This research resulted in a top-scoring group of 12 IG1 Safeguards. We validated this **"Transformative Twelve"** via independent IU and Purdue subject matter expert analysis, confirmed the very high presence of these Safeguards in other standards (*e.g.*, NIST's), compared to the results of a recent NC State University study[12] that followed a similar methodology to the CIS Community Defense Model v2.0, and ultimately conducted a detailed reanalysis[13].

As a result, we have high confidence that the core set of specific controls we're assessing are truly fundamental and impactful. This is not to say that these are the only controls that are worth implementing. Moreover, much-needed future research may result in a somewhat different top-scoring group. However, in the context of a cybersecurity landscape where some "standards" include hundreds of controls, and most lack prioritization or evidentiary grounding, we see building real confidence in any subset as a victory for practicality.

---

[6] https://www.cisecurity.org/controls/cis-controls-faq.
[7] https://www.cisecurity.org/controls/implementation-groups/ig1.
[8] https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene.
[9] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0.
[10] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2021; https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.
[11] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight.
[12] * "An investigation of security controls and MITRE ATT&CK techniques," Md Rayhanur Rahman & Laurie Williams, 1 Nov 2022, arXiv:2211.06500v1, available at https://arxiv.org/pdf/2211.06500.pdf.
[13] This recent reanalysis resulted in two Safeguards (6.3 and 11.4) joining the top-scoring group. We are now assessing those and will begin covering their results and trends in future reports.

Table 1: The Transformative Twelve

2.3	Address Unauthorized Software
3.3	Configure Data Access Control Lists
3.4	Enforce Data Retention
4.1	Establish and Maintain a Secure Configuration Process
4.7	Manage Default Accounts on Enterprise Assets and Software
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
6.3	Require MFA for Externally-Exposed Applications
6.4	Require MFA for Remote Network Access
6.5	Require MFA for Administrative Access
10.1	Deploy and Maintain Anti-Malware Software
10.2	Configure Automatic Anti-Malware Signature Updates
11.4	Establish and Maintain an Isolated Instance of Recovery Data

To the Transformative Twelve we added a small number of additional IG1 Safeguards based on the Cybertrack Team's analysis of particular relevance to local governments, contemporary attack patterns (*e.g.*, prominence of ransomware), as well as inventory controls that scored lower in the CIS Community Defense Model for methodologically technical reasons (as opposed to any evidence that they are not truly critical). Finally, we added an additional handful of Safeguards that map to "cybersecurity best practices" emphasized in the federal State and Local Cybersecurity Grant Program[14] if not already included via our research. All said, Cybertrack is assessing 27 of CIS's 153 Safeguards, including 24 of IG1's 56.

Implementation Ratings. Much of the Results and Analysis that follow focus on implementation ratings for the Musts and Safeguards we assess. We developed a rating rubric for each Must and Safeguard we assess, as well as common implementation rating scale:

> **Optimizing**: The evidence showed that the organization is implementing the fundamental elements of this Must or Safeguard, and has taken action to fortify or refine its implementation (*e.g.*, for greater effectiveness, efficiency, or programmatic resilience).
>
> **Implementing**: The evidence showed that the organization is implementing the fundamental elements of this Must or Safeguard, with no significant gaps across its environment.
>
> **Developing**: The evidence showed that the organization is implementing some, but not all of the fundamental elements of this Must or Safeguard, *or* there exist significant gaps in the implementation within the environment.
>
> **Not Implementing**: Discovery produced little or no evidence that the organization is implementing any of the fundamental elements of this Must or Safeguard.

[14] https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program.

Not Rated: We use this when we do not provide a rating for a Must or Safeguard. Reasons may include not having enough information to be confident in our rating, or the Must or Safeguard being inapplicable to the organization receiving the assessment.

"Fundamental elements" are the minimum requirements for us to confidently say that the assessed organization "is implementing" the Must or Safeguard.

A "significant gap" is a gap in the implementation of a Must or Safeguard of sufficient scale or concern as to warrant further consideration. These include cases where risk presented by the gap is not mitigated by other Must or Safeguard implementations. The "as to warrant further consideration" language is intentional: The identification of a significant gap does not necessarily mean that gap should or necessarily can be closed. An example might be multi-factor authentication being implemented for remote access, but only for a small subset of the relevant systems.

When evaluating the evidence provided, we follow these guidelines:

1. We assume that respondents' factual statements are truthful and accurate.
2. We assume that respondents have not intentionally omitted important facts.
3. Unless called for explicitly, we do not consider respondents' statements of opinion when determining implementation ratings.

2.2 Approach to Data Analysis

Data collected for analysis are taken from completed WDRs, final implementation ratings for each Must and Safeguard for each assessed entity, and publicly-available information. Where multiple layers of data are captured for analysis, multiple worksheets within the workbook are used to store data. Those data are related to each other using referencing formulae within the workbook.

Some of the more structured or categorical data (*e.g.*, implementation ratings, entity type, municipal spending information) were used directly in analysis. Most of the data used, including those from WDRs and assessment ratings, were coded to facilitate our analysis. Our analysis relied heavily on assessment teams' assessment ratings, which were coded as shown in the table below.

Table 2: Implementation Ratings Coding System

Rating	Code
Not Rated	N/A
Not Implementing	0
Developing	1
Implementing	2
Optimizing	3

We adopted a numerical coding method for the rating system, enabling us to generate rating metrics.[15] These metrics included intermediary aggregate scores for both the assessed Trusted CI Musts and the assessed CIS Safeguards, and, ultimately, an overall assessment rating score for each entity for both the Musts and the Safeguards. To handle the local government free-form responses collected in the WDR, our team developed coding systems to preprocess this qualitative data for analysis. Data entered into the analysis workbook were checked by the analyst entering the data, then re-checked by another member of the team before analysis began.

We began our analysis by generating basic descriptive statistics (mean and variance) for each implementation rating across all entities. The team also generated a bar graph for each Must and Safeguard that showed the percentage of entities that achieved each implementation rating. We performed basic statistical comparisons. The team validated calculations and results by having a second team member validate the formulae used in calculations. We performed more advanced statistical comparisons, such as regression and ANOVA analyses, using SAS version 9.4.

3 Results

This section provides an overview of the aggregated assessment results of the first 23 local government entities to participate in the Cybertrack program. We begin with the basic characteristics of the local government population and sample-to-date [Table 3] and summarize the aggregated results of the implementation ratings across the Musts and Safeguards we assess [Figures 1 & 2]. Finally, we provide results of some of the team's basic statistical analyses.

According to the 2022 United States Public Sector Annual Survey and Census of Governments,[16] 2,649 local government entities exist in the State of Indiana. These entities include: "counties, cities, townships, special districts (such as water districts, fire districts, library districts, mosquito abatement districts, and so on), and school districts."[17] 1,662 were general purpose governments (eg. counties, cities, and other municipalities)[18] that served as the primary governing entity. The remaining 987 local governmental entities include K-12 school districts and special service governing bodies, among others. The 2022 United States Census estimates Indiana's population at 6,833,037 people.

Data collected as part of this assessment include descriptions of assessed entities based on type of local governmental entity, and population. Table 3 below classifies assessed entities by the type of local entity. Nearly all (22 of 23) of the entities we've assessed since the March 2023 start of this program were county or municipal governments. The county, municipal, and township governments assessed by the Cybertrack program to date represent 0.78% of Indiana's general purpose governments. Populations serviced by assessed entities ranged from 2,100 people to 385,000.[19] Eight assessed entities were rural as defined by The Department of Homeland Security (DHS) Notice of

[15] We do not provide numerical scores to assessed entities as part of their assessment report. For individual organizations, these scores could be misleading for a number of reasons, including the fact that not all Musts and Safeguards are equally powerful. The purpose of the numerical scoring system is solely to facilitate our analysis of aggregate results across the assessed population sample.
[16] https://data.census.gov/table/GOVSTIMESERIES.CG00ORG01?q=local+governments+in+Indiana.
[17] https://www.census.gov/programs-surveys/gus/about.html.
[18] https://www2.census.gov/programs-surveys/gus/datasets/2017/2017_gov_org_meth_tech_doc.pdf.
[19] https://data.census.gov.

Funding Opportunity (NOFO) Fiscal Year 2022 Homeland Security Grant Program[20] because they serve a population of 50,000 people or fewer. Average yearly spending ranged among assessed entities from approximately $11.5 million dollars to nearly $1.5 billion dollars.[21]

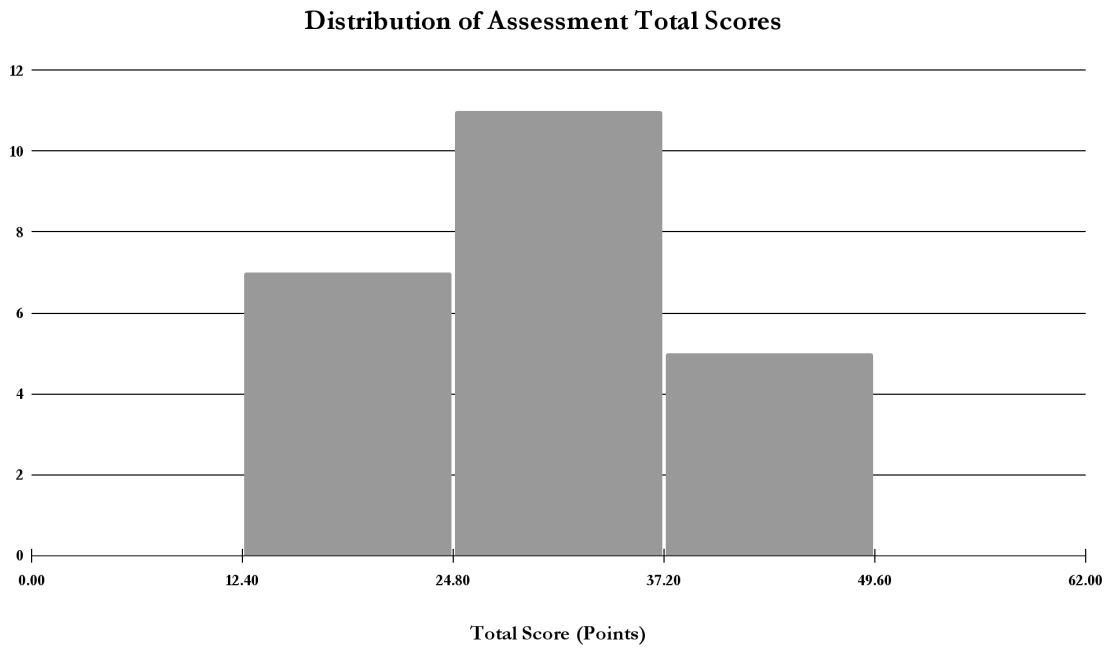
Table 3: Number of Assessed Entities by Type of Entity

Type of Entity	Number of Entity Type
County Government	12
Municipal (City/Town) Government	10
Township Government	0
K-12 School District	0
Library	1
Other	0
Total	**23**

Basic descriptive analysis of the implementation ratings follows and provides additional context to the data displayed in Figure 1 above. Using the implementation ratings coding system, total scores for assessed entities ranged from 13 to 41 points out of 93 possible points. It is important to note that an entity would need to be rated as "Optimizing" on all 31 assessed Musts and Safeguards, as defined in the Methodology section of this report, to earn 93 points. If an entity earned an "Implementing" rating on the 31 assessed Musts and Safeguards, that entity would receive a total score of 62 points (a very significant milestone to hit, representing the top end of the graph below). An entity that received all "Developing" ratings would receive a total score of 31. The following results and analysis discuss general trends in the assessment data, but results of individual assessments varied widely. Cybersecurity postures among assessed entities are likely to look very different both when comparing a score of 13 to 41, as well as when comparing two entities with more similar total scores. The graph below shows the distribution of assessment total scores.

[20] https://www.fema.gov/grants/preparedness/homeland-security/fy-22-nofo
[21] https://gateway.ifionline.org/report_builder/

Chart 1: Distribution of Assessment Total Scores (Number of Entities (Y) x Ranges of Total Score)



The average total score for all assessed entities was 29.90 out of 93 possible points, which averages to 0.96[22] points for each of the 31 assessed Musts and Safeguards. Meaning, in general, entities averaged slightly below a Developing implementation rating. For the 6 assessed Trusted CI Musts, entities averaged 5.93 points, or 0.99 points per Must. CIS Safeguards only, entities averaged 23.93[23] points across 25 assessed Safeguards, or 0.96 points per Safeguard. Additionally, none of the assessed entities received a rating of "Implementing" or better for the following assessed controls:

- CIS 2.1: Establish and Maintain a Software Inventory
- CIS 2.2: Ensure Authorized Software is Currently Supported
- CIS 2.3: Address Unauthorized Software
- CIS 4.1: Establish and Maintain a Secure Configuration Process
- CIS 7.1: Establish and Maintain a Vulnerability Management Program
- CIS 8.1: Establish and Maintain an Audit Log Management Program

These results serve as the basis for our analysis of the cybersecurity posture of Indiana's local entities that have thus far participated in the Cybertrack program in the next section.

[22] Three assessed entities received no rating for CIS Safeguard 2.1. One assessed entity received no rating for CIS Safeguard 4.1.
[23] Ibid.

4 Analysis

In this section, we provide our analysis of results from 23 assessed entities that represent the early program participants, including those in the pilot stage, completed between March and November 2023. We start our analysis with a general characterization of assessment results (Section 4.1). Next, we discuss a sampling of specific results that are noteworthy, either as reasons for optimism or concern, in terms of the assessed Trusted CI Musts (Section 4.2) and CIS Safeguards (Section 4.3). Finally, we present two particularly strong correlations present in these data (Section 4.4). This is an early report of results and analysis that may or may not capture the trends in the greater populations described in Section 3 above.

4.1 General Characterization of Assessment Results

The Cybertrack Team's analysis focuses on Implementation Ratings data generated from assessments. As described in the Methodology section above, Cybertrack assessments evaluated a small number of Musts and Safeguards identified as most powerful and fundamental through the team's research. On average, assessed entities received slightly less than one point (0.96) per assessed Must and Safeguard out of the 3 points possible. This means that, in general, entities averaged slightly below a Developing implementation rating. Additionally, none of the assessed Musts or Safeguards individually averages a score of 2 or greater, which would represent an average status of "Implementing."

We also evaluated demographic data for statistical significance of correlation to total assessment scores. For these analyses, we analyzed the following data against total score:

- Total population
- Total spending
- Use of state cybersecurity resources
- Type of organization (city, town, county, etc.)
- Number of users
- Number of IT personnel employed
- Number of IT endpoints
- Whether the entity experienced a cybersecurity incident in the past three years

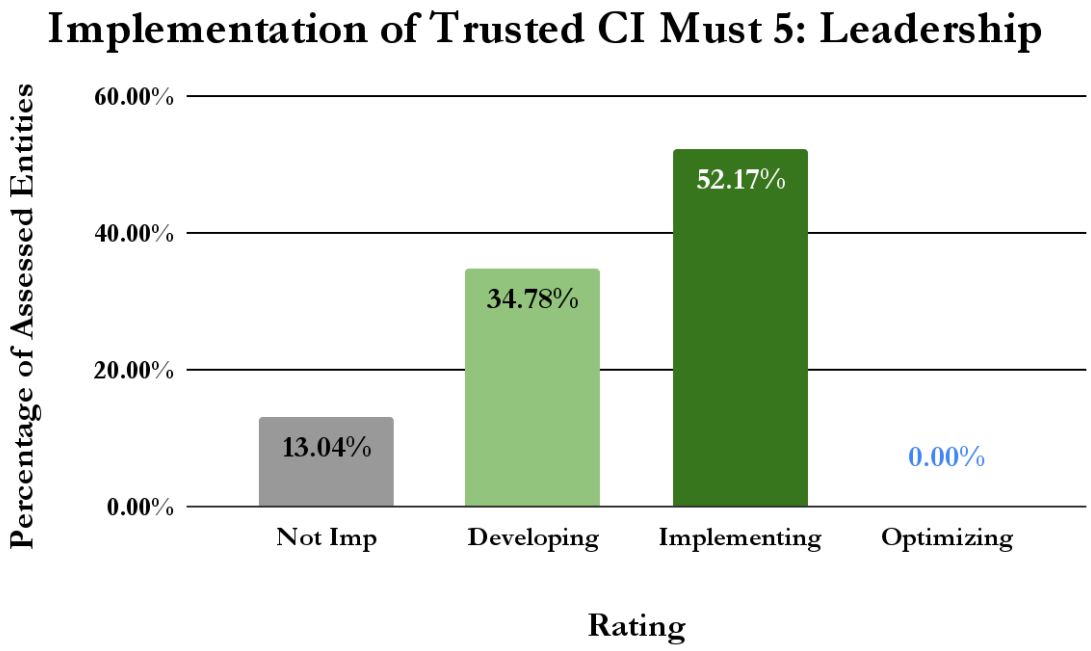
The only demographic data that produced a statistically significant correlation to total score was experience with cybersecurity incidents. This relationship is discussed in more detail in section 4.4 "Early Correlations" later in this report.

4.2 Noteworthy Results: Trusted CI Musts

As noted in Section 2.1 above, the Trusted CI Musts evaluate the organizational cybersecurity fundamentals, or programmatics, driving entities' cybersecurity efforts. Cybertrack assessments evaluate 6 of the 16 Musts, listed in Appendix A. The most encouraging result from our evaluation of the Musts described the involvement of leadership in cybersecurity decision making. Assessed entities averaged 1.39 points on Must 5, Leadership. This average implementation rating on Must 5

exceeded the average rating of other Musts, as well as 25 of 28 assessed Safeguards. More than half of assessed entities (52.17%) received an "Implementing" rating on this Must, while 34.78% received a "Developing" rating. Two assessed entities received a rating of "Not Implementing". The chart below illustrates the ratings distribution from Must 5.

Chart 2: Implementation Ratings Distribution: Must 5 (Leadership)

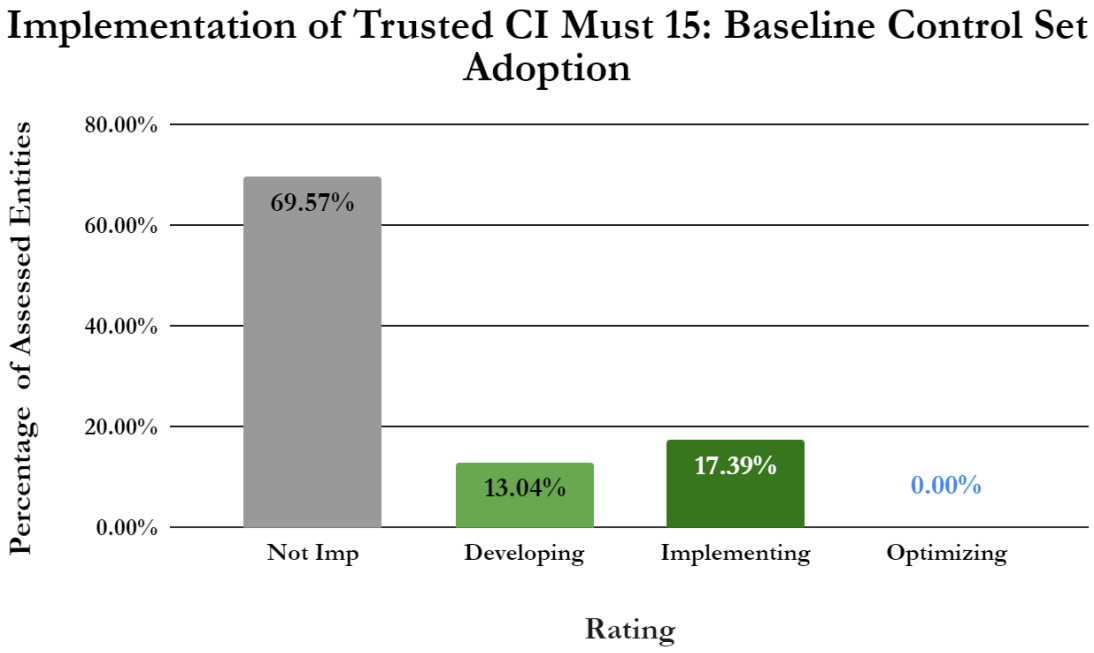


To address cybersecurity competently, senior leadership must be involved in cybersecurity decision making. Organizational leaders are the primary agents of the organizations for which they work, representing the organization to the outside world. They are ultimately responsible for the organization, and are best positioned to bear the burdens of tough decisions about risk taking and risk reduction. No job roles are more directly and holistically connected with the organization's mission than those of its leadership. They ultimately control the allocations of resources, budget, and personnel to support the cybersecurity program.The causes of these relatively positive results are not clear, but they may be a result of increasing awareness of the importance of cybersecurity, increasing frequency of successful cyber attacks on local governments[24], and/or the relatively small nature of local government entities where most if not all expenditures require senior leadership engagement. Regardless, we view the relatively high distribution of implementation ratings for Must 5 as a point of strength and reason for optimism in this analysis.

On the other end of the spectrum, few assessed entities had adopted a baseline set of cybersecurity controls (Must 15). Assessed entities averaged only 0.48 points on this Must. As shown in Chart 3 below, nearly 70% were not implementing this Must. Less than 20% had formally adopted a baseline set of cybersecurity controls, such as the CIS Safeguards or NIST Cybersecurity Framework.

[24] Mahendru, P. *The State of Ransomware in State and Local Government 2023*. Sophos. https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-government.

Chart 3: Implementation of Trusted CI Must 15: Adoption of a Baseline Control Set



Control set adoption is critical to a well-functioning cybersecurity program. An adopted framework provides a common language that facilitates discussions of cybersecurity concepts and topics throughout the organization. When creating cybersecurity plans and budgets, an adopted control set helps to ensure that executive and IT leaders can translate cybersecurity risks into technical, physical, and policy solutions that mitigate those risks. A control set also facilitates assessment of the organization's cybersecurity posture. Cybersecurity assessment provides a baseline understanding of an organization's cybersecurity posture, gaps in controls, and when performed regularly over time, information about an organization's progress in reducing cybersecurity risk.

Our overall evaluation of the state of cybersecurity programmatics among assessed entities considered the results from Musts 5 and 15 presented above, as well as the average score on all assessed Musts, the mode for each Must implementation rating, and the relationship between an entities' total Musts scores and total Safeguards scores. Assessed entities averaged only 5.26 points out of 18 possible across all assessed Musts. Unfortunately, Must 5 is the only assessed Must where the most commonly achieved rating was "Implementing." We most frequently evaluated Musts requiring an established cybersecurity lead role (Must 7), implementation of a formal cybersecurity policy (Must 9), and the formal designation of personnel to cybersecurity responsibilities (Must 13) as "Developing." Assessed entities most frequently achieved a "Not Implementing" rating for not having a cybersecurity budget (Must 12), and for not adopting a cybersecurity control set (Must 15). **These data indicate that assessed entities' leaders are aware of cybersecurity as a source of risk to their organizations, but that they have a lot of work to do to build formal cybersecurity programs to address cybersecurity risks.**

Entities' total scores on the six assessed Trusted CI Musts are a significant predictor of entities' total

Safeguard scores. That is, with 23 entities assessed, the entities that have made more progress developing formal cybersecurity programs have made more progress implemented technical cybersecurity Safeguards (α=0.05, p=0.01, r^2=0.26). In the next section, we discuss assessed entities' implementation of technical Safeguards. Total scores on Safeguards among assessed entities range from 10 points to 34 points out of 75 possible points.

4.3 Noteworthy Results: CIS Safeguards

Implementation ratings for assessed CIS Control 10 "Malware Defenses" Safeguards were the two highest rated by mean score among all 25 assessed CIS controls, both of which are members of the "Transformative Twelve". The mean score for CIS Safeguard 10.1, which requires assessed entities to "Deploy and Maintain Anti-Malware Software"[25] was 1.74 points. The mean score for CIS Safeguard 10.2, "Configure Anti-Malware Signature Updates"[26] was 1.17 points. The mode rating for both Safeguards was "Implementing" and none of the assessed entities received a "Not Implementing"rating on either Safeguard. Charts 4 and 5 below provide a graphical representation of implementation ratings for these safeguards.

[25] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 31.
[26] Ibid.

Chart 4: Implementation Ratings Distribution: CIS Safeguard 10.1: Deploy and Maintain Anti-Malware Software

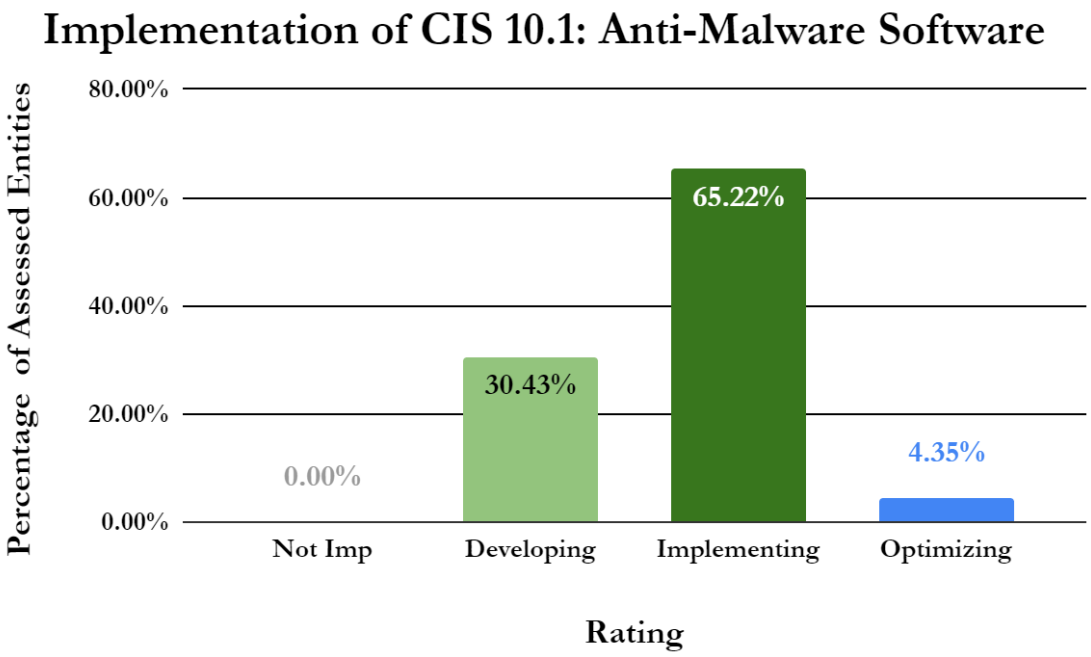
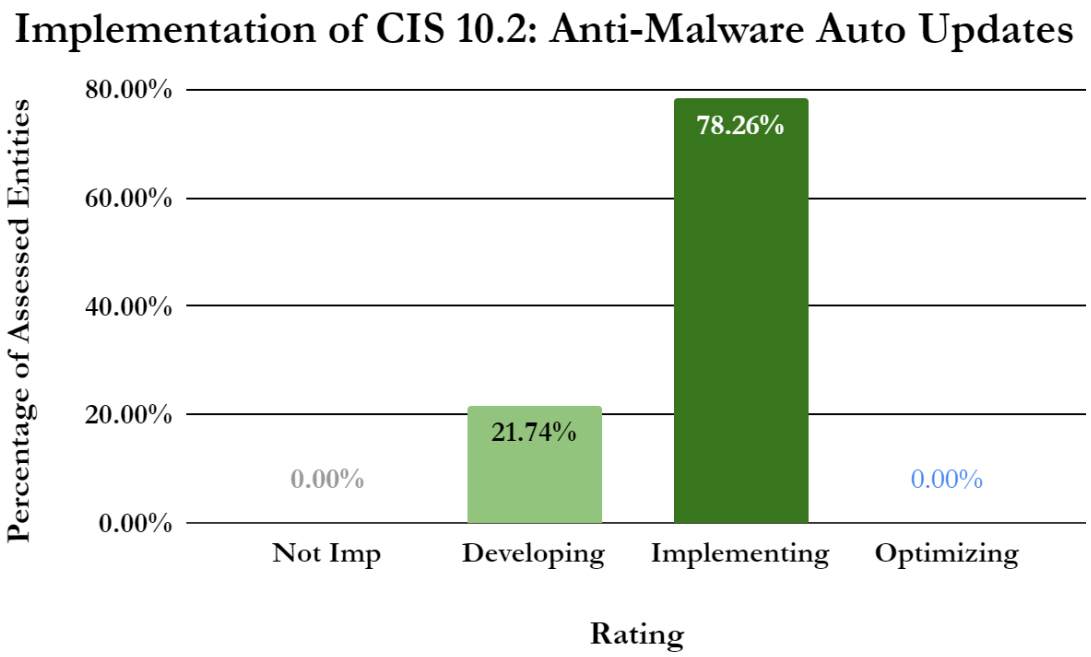


Chart 5: Implementation Ratings Distribution: CIS Safeguard 10.2: Configure Anti-Malware Signature Updates



Ransomware incidents have been costly to local governments. Attacks on Atlanta[27] and Baltimore[28] are prominent examples but Indiana local government entities and K-12 school districts have also been extorted through ransomware.[29] [30] Organizations that implement and maintain anti-malware software are better protected against ransomware infection than those without anti-malware software. Relatively high ratings and lack of "Not Implementing" ratings for assessed entities on CIS Safeguards 10.1 and 10.2 represent a point of strength in Indiana local entities' cybersecurity postures.

Conversely, overall ratings for Safeguards related to software inventory and control (CIS Control 2), log management (CIS Control 8), vulnerability management (CIS Control 7), and cybersecurity incident response (CIS Control 17) indicate that assessed entities are struggling to develop those Safeguards. Assessed entities had the lowest incidence of employing controls related to building software inventories and controlling software assets. The Cybertrack Team assesses three CIS Safeguards on this topic: Safeguard 2.1, "Establish and Maintain a Software Inventory",[31] Safeguard 2.2, "Ensure Authorized Software is Currently Supported",[32] and Safeguard 2.3, "Address Unauthorized Software",[33] another member of the Transformative Twelve. The mean Implementation Rating scores for these three controls were 0.50 points, 0.47 points, and 0.53 points, respectively, indicating that few assessed entities were even developing implementations related to these Safeguards. High percentages of "Not Implementing" ratings among assessed entities on Control 2 Safeguards and zero "Implementation" ratings on any of these three Safeguards further illustrate assessed entities' lack of software inventory and control.

[27] https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack
[28] https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html
[29] https://cyberscoop.com/indiana-ransomware-la-porte-county/
[30] https://www.nwitimes.com/news/local/education/crown-point-schools-victim-of-ransomware-attack/article_1ee07b98-57ff-11ee-bb41-5fe43ab302d8.html
[31] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 12.
[32] Ibid.
[33] Ibid.

Chart 6: Implementation Ratings for CIS Safeguard 2.1, Software Inventory

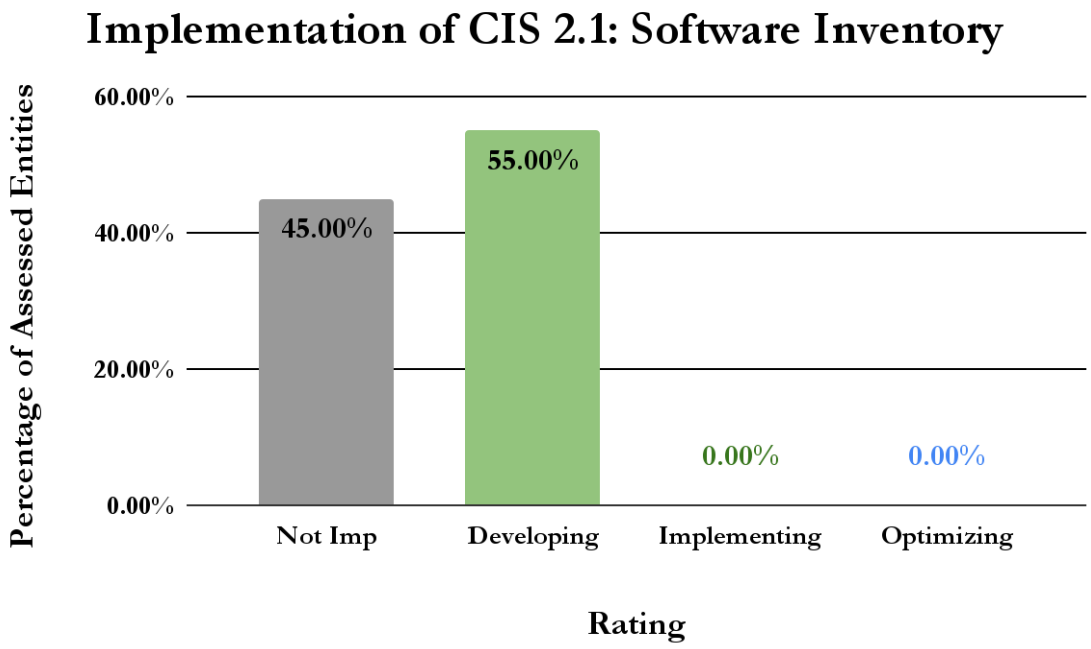


Chart 7: Implementation Ratings for CIS Safeguard 2.2, Ensure Authorized Software is Supported

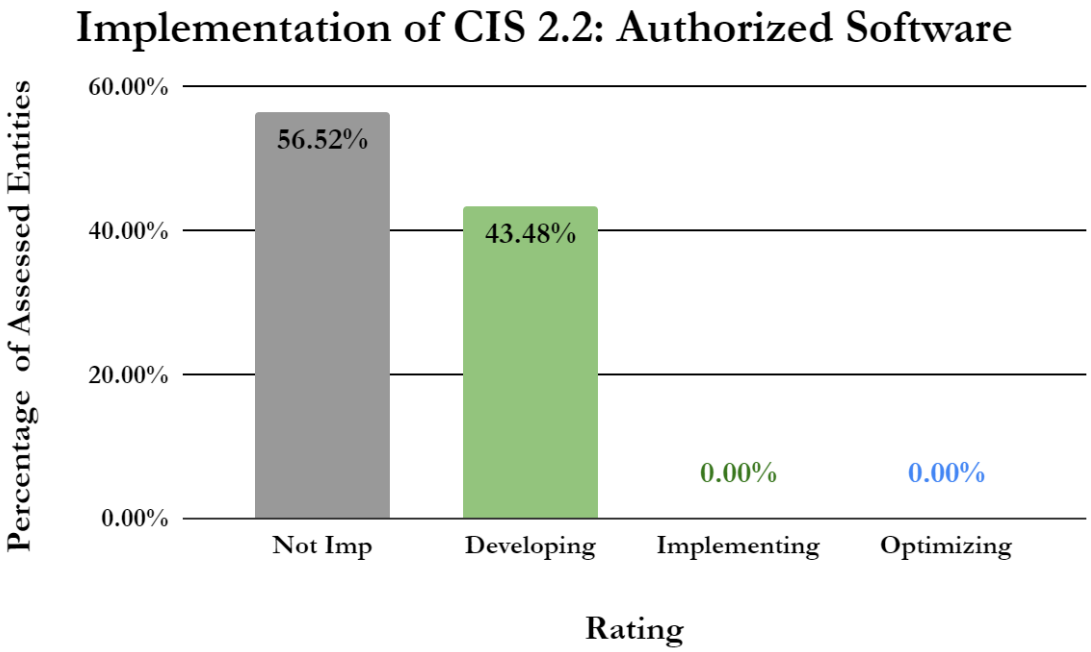
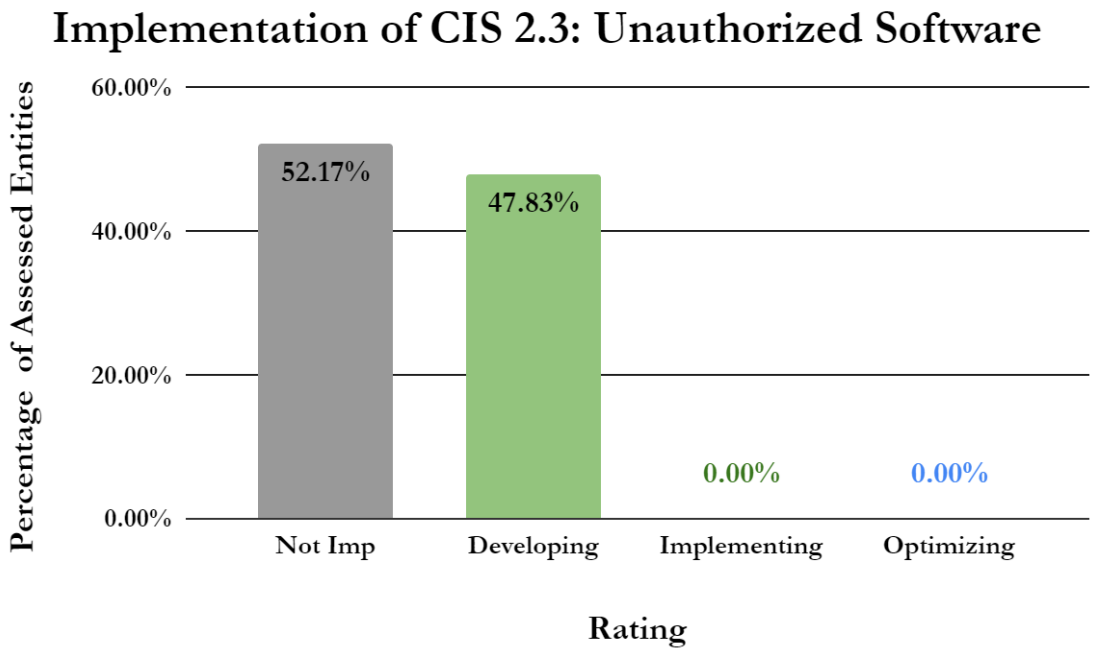


Chart 8: Implementation Ratings for CIS Safeguard 2.3, Address Unauthorized Software

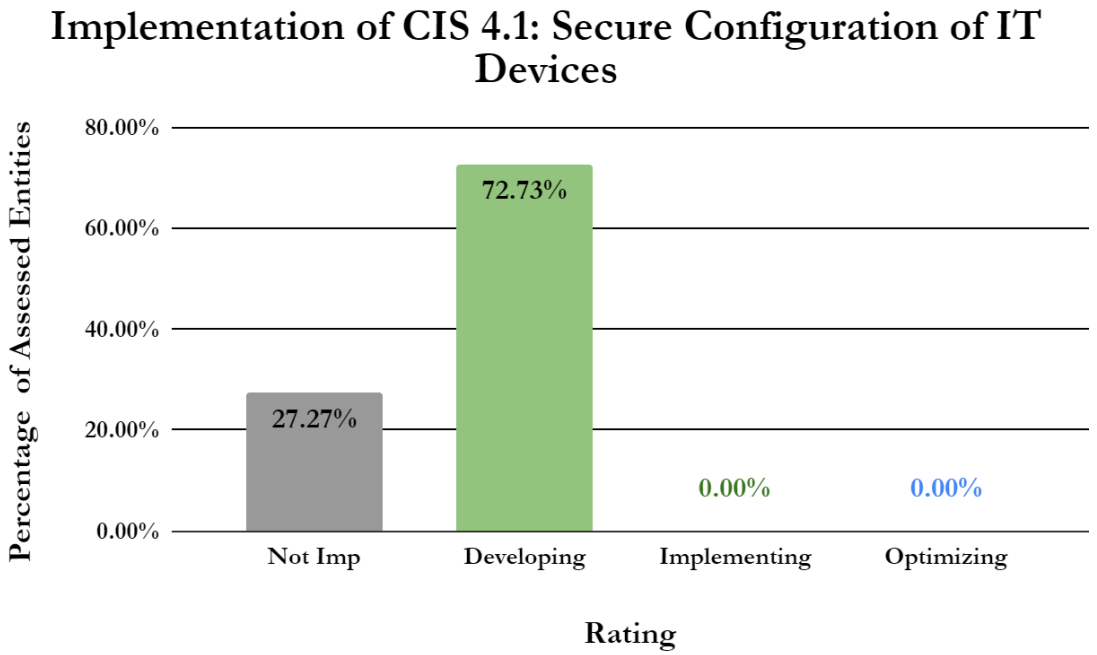


All three of these Safeguards ranked among the bottom five assessed Safeguards by mean score. Like the CIS Safeguards 10.1 and 10.2 discussed above, Safeguards 2.1, 2.2, and 2.3 also impact an organization's ability to prevent malware infections. When unauthorized software is installed or when authorized software is not properly maintained, software retains vulnerabilities on computers and networks that facilitate cybersecurity attacks.

Organizations can manage software vulnerabilities, in part, by ensuring strong configuration processes for IT assets as detailed in CIS Safeguard 4.1.[34] Our evaluation of Safeguard 4.1 produced results similar to those for Safeguards 2.1, 2.2, and 2.3. Most commonly, assessed entities received a "Developing" implementation rating on Safeguard 4.1, but 27% were rated as "Not Implementing". None received an "Implementing" rating, which kept the mean score low (0.72). The chart below represents assessed entities' ratings on Safeguard 4.1 graphically.

[34] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 16.

Chart 9: Implementation Ratings for CIS Safeguard 4.1: Establish and Maintain a Secure Configuration Process.

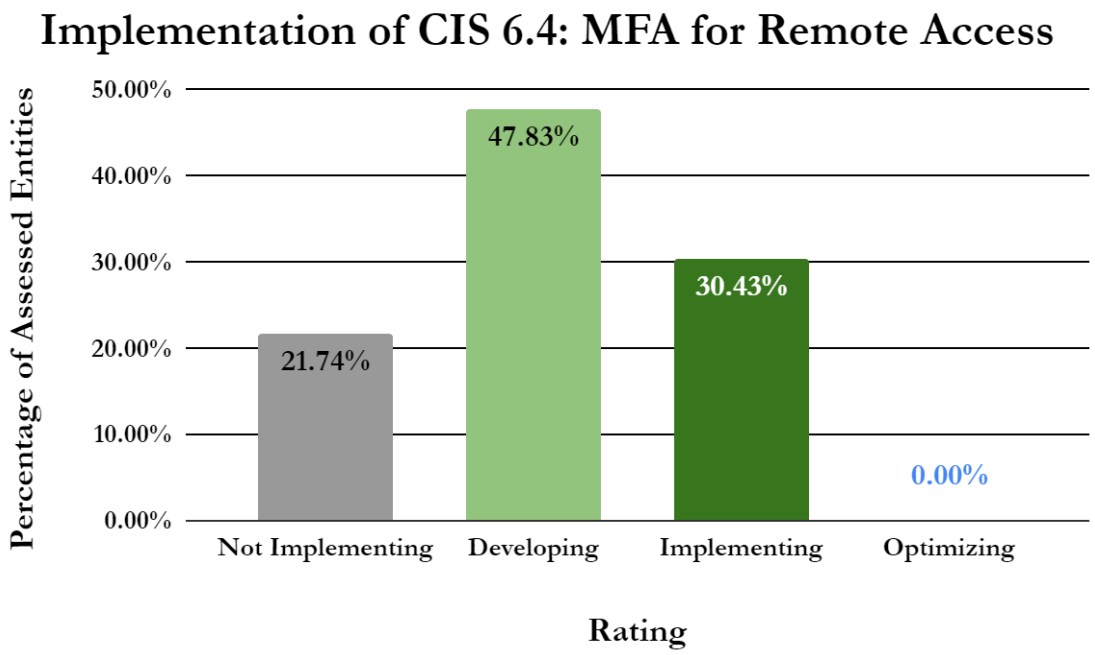


Generally low implementation ratings for Safeguard 4.1 are concerning because, lacking a robust process to ensure repeatability of strong asset configurations within an organization, the organization is likely to put less secure devices into operation. These devices are unnecessarily vulnerable to cyberattack. Low implementation ratings on this Safeguard are also concerning in the context of low implementation ratings on CIS Control 2, "Inventory and Control of Software Assets".[35] Weaknesses in device configuration can, for example, allow users to install vulnerable or malicious software or remove protective software, which may create additional vulnerabilities that allow devices to be compromised, and the organization to be victimized by cyberattack.

Substantial empirical research, including that resulting in the identification of the Transformative Twelve Safeguards indicates multi-factor authentication is an especially powerful control in preventing successful cyberattacks. Assessed entities have mixed results implementing MFA in remote access processes. Cybertrack assesses entities' implementation and use of multi-factor authentication through CIS Safeguards 6.4, "Require MFA for Remote Access" [36] and 6.5, "Require MFA for Administrative Access,"[37] and will be adding 6.3 "Require MFA for Externally-Exposed Applications" to future assessments and reporting. 40% of assessed entities were implementing MFA for remote access. 46.67% of entities were "Developing" MFA for remote access. 13% of assessed entities were not implementing MFA for remote access. In sum, less than 30% of participating organizations were fully implementing MFA on remote access at the time of assessment, but more than 40% of them had made at least some meaningful progress toward implementation, as shown in the chart below.

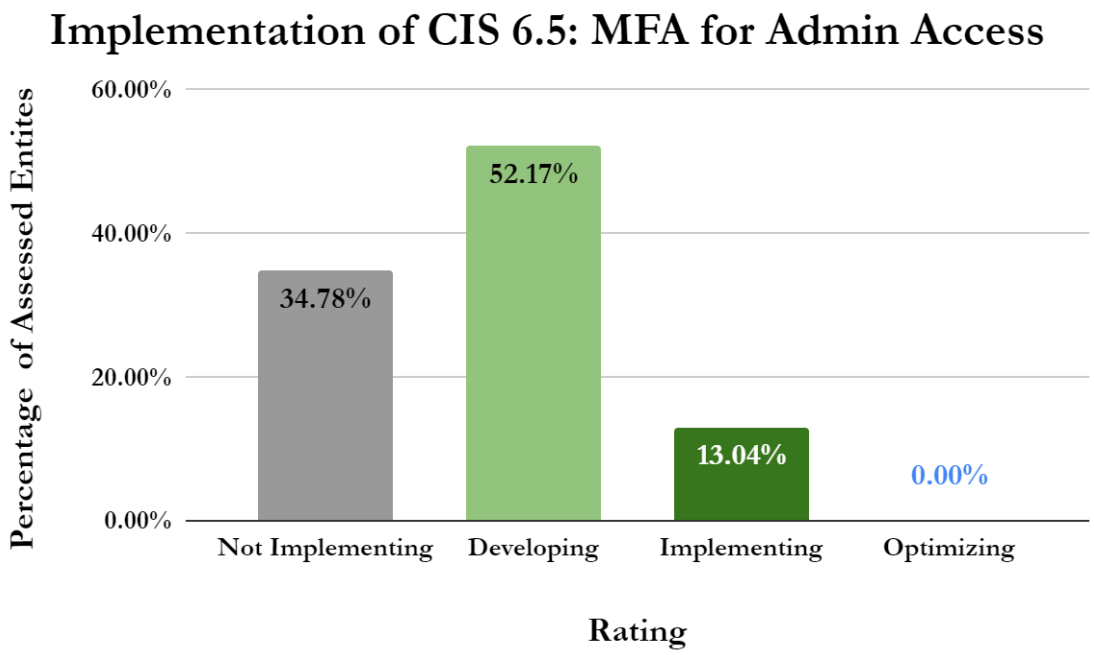
[35] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 10.
[36] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 22.
[37] Ibid.

Chart 10: Distribution of Implementation Ratings for CIS Safeguard 6.4: Require MFA for Remote Network Access



The assessed entities have been even less successful in requiring MFA for administrative access to their systems. Though more than half of assessed entities were "Developing" this Safeguard, a startling 46% were not implementing MFA for administrative access. Relatively low implementation of MFA on accounts that have the most powerful access to organizational systems is quite concerning, especially given the enormous power MFA has as a control to prevent unauthorized access, and therefore, prevent successful cybersecurity attacks. Chart 11 displays these results.

Chart 11: Distribution of Implementation Ratings for CIS Safeguard 6.5: Require MFA for Administrative Access



4.4 Early Correlations

One of Cybertrack's primary goals is to inform Indiana's local government cybersecurity policy and strategy. Because the program has so far assessed only a small number of local governments, our ability to make accurate inferences about that population is limited. Despite this limitation, two correlations stand out as statistically significant in this early stage of our work.

First, our analysis shows that an entity's total score on assessed Trusted CI Musts is significantly positively correlated to its total score on assessed CIS Safeguards. That is, where entities received higher total scores on Trusted CI Musts, those entities generally received correspondingly higher scores on CIS Safeguards, and vice versa (α=0.05, p=0.01, r^2=0.26). Among the Musts, Must 12: Cybersecurity Budget (α=0.05, p=0.003, r^2=0.35), Must 13: Personnel (α=0.05, p=0.003, r^2=0.35), and Must 15: Baseline Control Set (α=0.05, p=0.01, r^2=0.25) were significantly correlated with an entity's total score on assessed CIS Safeguards. These statistics may indicate the power (if not necessity) of these organizational fundamentals in enabling the implementation of the more tactical, more technical controls that are frequently the focus of cybersecurity standards. We argue that organizations cannot successfully put the technical cart before the organizational horse, and this correlation provides some validation.

The second early stand-out trend is that entities that report experiencing a cybersecurity incident in the past three years are implementing more of the Musts and Safeguards we assess. Using an ANOVA test, prior incidents were significant predictors of total score (α=0.05, p=0.02, r^2=0.24). This result supports an anecdotally common assertion across the cybersecurity community: Many organizations find ways to invest in cybersecurity only after they themselves experience an incident, even in the face of evidence that similar organizations are falling victim.

5 Conclusion

One of Cybertrack's primary goals is to inform Indiana's local government cybersecurity policy and strategy. This report supports that goal. Considering Cybertrack only assesses cybersecurity practices that are known to be among the most powerful, these early results are sobering. Indiana's local government entities have a long way to go on basic cybersecurity capability, and they most certainly need help.

Our early results and analysis based on Cybertrack's first 23 assessments show that organizational leadership is involved in cybersecurity decision making in about half of assessed organizations. Based on the 35% of assessed entities who are Developing on this Must, we are hopeful that more organizations' leaders will become involved in cybersecurity decision making and soon. As leadership becomes more involved in organizational cybersecurity, our early analysis suggests that they should focus on building a cybersecurity-specific budget (Must 12), assigning people to cybersecurity tasks (Must 13), and adopting a baseline cybersecurity control set, or framework, to gauge cybersecurity posture, find gaps, and monitor progress (Must 15). Strong cybersecurity programmatics provide a basis for prioritizing cybersecurity investment. Indiana local government entities should prioritize these organizational fundamentals. They are necessary to support sound decision making and cybersecurity investment.

These early results also indicate most Indiana local government entities are struggling to implement even the most fundamental, powerful controls. Our research narrowed the 153 CIS Safeguards down to a list of 27, including 12 of the most empirically-proven as powerful. Investing in these Safeguards, certainly to include the Transformative Twelve discussed in Section 2.1 (Assessment Methodology), will lead to significant reductions to organizations' cybersecurity risk exposure. Results from "Inventory and Control of Software Assets" (CIS Control 2) Safeguards provide a particularly extreme example of these struggles. No assessed entity received an "Implementing" rating on Safeguards 2.1, 2.2, or 2.3. Respectively, 45%, 57%, and 52% of assessed entities were "Not Implementing" these safeguards. This control provides particularly significant opportunities for improvement of cybersecurity postures through the development of cybersecurity controls, but its ratings distribution is representative of several safeguards we assessed. Moreover, growing evidence supporting the particular power of secure configurations (CIS Control 4) and multi-factor authentication (CIS Control 6) suggest that local entities should focus particular attention on these. The community should prioritize all the Safeguards covered in this assessment, with particular attention to the most proven: These include the Transformative Twelve (see the Executive Summary's Figure 2 and Section 2.1).

Looking ahead, we anticipate publishing aggregate results reports like this one regularly. We will focus on clarifying, detailing, and (where necessary) correcting our analysis of trends as the number in our sample set grows. We'll increasingly be able to report on correlations among Must and Safeguard implementation ratings and factors such as budget, population size, and type of entity, as well as draw precise conclusions about barriers to progress. And, we'll increasingly be able to report on impact, change, and challenges, as organizations we've assessed report back to us on progress. We welcome feedback on this report, and ideas for how to maximize the value of future Cybertrack reporting to the community.

Appendix A: Musts and Safeguards Assessed

Trusted CI Framework Musts (assessing 6 of 16)

Must 5: Leadership
Organizations must **involve leadership** in cybersecurity decision making.
Must 7: Cybersecurity Lead
Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
Must 9: Policy
Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policies**.
Must 12: Budget
Organizations must establish and maintain a **cybersecurity budget**.
Must 13: Personnel
Organizations must allocate **personnel** resources to cybersecurity.
Must 15: Baseline Control Set
Organizations must adopt and use a **baseline control set**.

CIS Safeguards (assessing 27 of 153, each from Implementation Group 1 unless otherwise noted)

CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
CIS 2.1: Establish and Maintain a Software Inventory
CIS 2.2: Ensure Authorized Software is Currently Supported
CIS 2.3: Address Unauthorized Software ‡
CIS 3.3: Configure Data Access Control Lists ‡
CIS 3.4: Enforce Data Retention ‡
CIS 3.10: Encrypt Sensitive Data in Transit (IG2 & IG3)
CIS 3.11: Encrypt Sensitive Data at Rest (IG2 & IG3)
CIS 4.1: Establish and Maintain a Secure Configuration Process ‡
CIS 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
CIS 4.3: Configure Automatic Session Locking on Enterprise Assets
CIS 4.6: Securely Manage Enterprise Assets and Software
CIS 4.7: Manage Default Accounts on Enterprise Assets and Software ‡
CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts ‡
CIS 6.3: Require MFA for Externally-Exposed Applications ‡ *
CIS 6.4: Require MFA for Remote Network Access ‡
CIS 6.5: Require MFA for Administrative Access ‡
CIS 7.1: Establish and Maintain a Vulnerability Management Process
CIS 7.3: Automated Operating System Patch Management
CIS 8.1: Establish and Maintain an Audit Log Management Process
CIS 10.1: Deploy and Maintain Anti-Malware Software ‡
CIS 10.2: Configure Automatic Anti-Malware Signature Updates ‡
CIS 11.1: Establish and Maintain a Data Recovery Process
CIS 11.4: Establish and Maintain an Isolated Instance of Recovery Data ‡ *
CIS 13.3: Deploy a Network Intrusion Detection Solution (IG2 & IG3)
CIS 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
CIS 17.7: Conduct Routine Incident Response Exercises (IG2 & IG3)

‡ In the Transformative Twelve. *See,* Section 2.1 for a discussion.
* Added as a result of recent re-analysis; we will begin covering their results and trends in future reports.