Driving Your Cybersecurity Program
An Overview of CYMETRICS

ATA FLEET CYWATCH PRESENTS
CYMETRICS
Powered by HudsonCyber

November 2021

Background What is "Cybersecurity"?

- Cybersecurity is ***NOT***:
  - Information Technology ("IT")
  - Compliance (e.g. ISO; NHTSA, NIST, etc.)
  - Solved by a "silver bullet" approach

- Cybersecurity ***IS***:
  - A sustained risk management activity
  - About cultural change and business transformation
  - Sustained collaboration
  - The mission of protecting the entire business (the Balance Sheet)
  - A responsibility that starts at the top

CYMETRICS and HudsonCyber

- Even though all types of industries are facing increased cybersecurity risk, there is a need for **continuously improving cyber-maturity in transportation** to prevent disruption of the global supply chain.
- **CYMETRICS provides management with a structured approach**, performance oriented means of identifying cyber risks, preparing a plan to close gaps, and tracking continuous improvement.
- HudsonCyber is **leveraging 30 years of transportation risk management** experience to provide a cyber solution for ship and port operators, and is making that solution available to trucking companies.

CYMETRICS Structured Like A Business

The CYMETRICS application provides transportation and logistics organization leadership with the sustained ability to analyze, benchmark, measure, and facilitate cybersecurity capability evolution across all the areas of your business.

Risk Management	Governance	Workforce & Training	Change Management
Situational Awareness	Information Sharing	Threat & Vulnerability Management	Commercial
Information Comm. Technologies (ICT)	Event & Incident Response	Physical	Cyber Program Management

CYMETRICS Makes Sense

HOURS SPENT PREPARING CYMETRICS CONTENT

Two senior resources worked together to update the assessment tool with the latest NHTSA, CTPAT, and DOD CMMC guidance to ensure the highest value for users.

Project hours from April to June with IT Executive and Cyber Expert	702

PROJECTED ASSESSMENT COSTS USING CYMETRICS

With CYMETRICS the team will have the ability to work together or independently, all of the progress can be tracked, recommendations for identified gaps are easily understood, and the cost of three years is less than 10% of the cost to organize the project in house.

CYMETRICS LICENSE*	$750
HOURS FOR SELF-ASSESSMENT ENTIRE TEAM FOR ONE DAY	8 $1,946.15
TOTAL COST FOR SELF-ASSESSMENT USING CYMETRICS**	**$2,696.15**

PROJECTED COSTS FOR INTERNALLY DELIVERED PROJECT

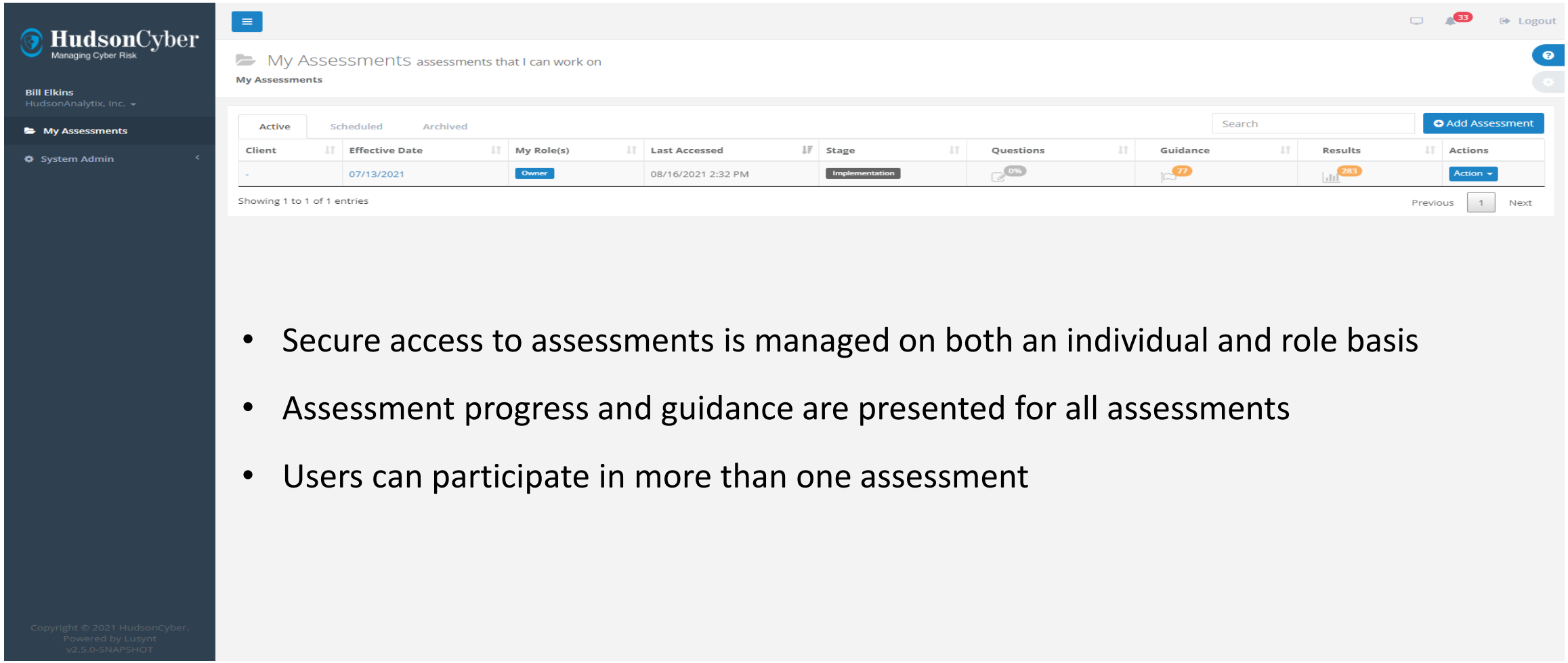
Based on HudsonCyber effort, completing this task in-house will not only require similar hours in duration, but with greater resources involved, and it will also take those resources away from daily operations.

RESOURCES	AVERAGE SALARY	COST PER HOUR
IT EXECUTIVE	$150,000	$72.12
APPLICATION DEVELOPMENT	$132,000	$63.46
NETWORK OPERATIONS	$113,000	$54.33
CISO OR SECURITY OFFICER	$111,000	$53.37
TOTAL HOURLY COST		$243
RESOURCE UTILIZATION		60%
INTERNAL PROJECT COST		**$102,465**

* Annual license $750 for non-ATA members and $500 for

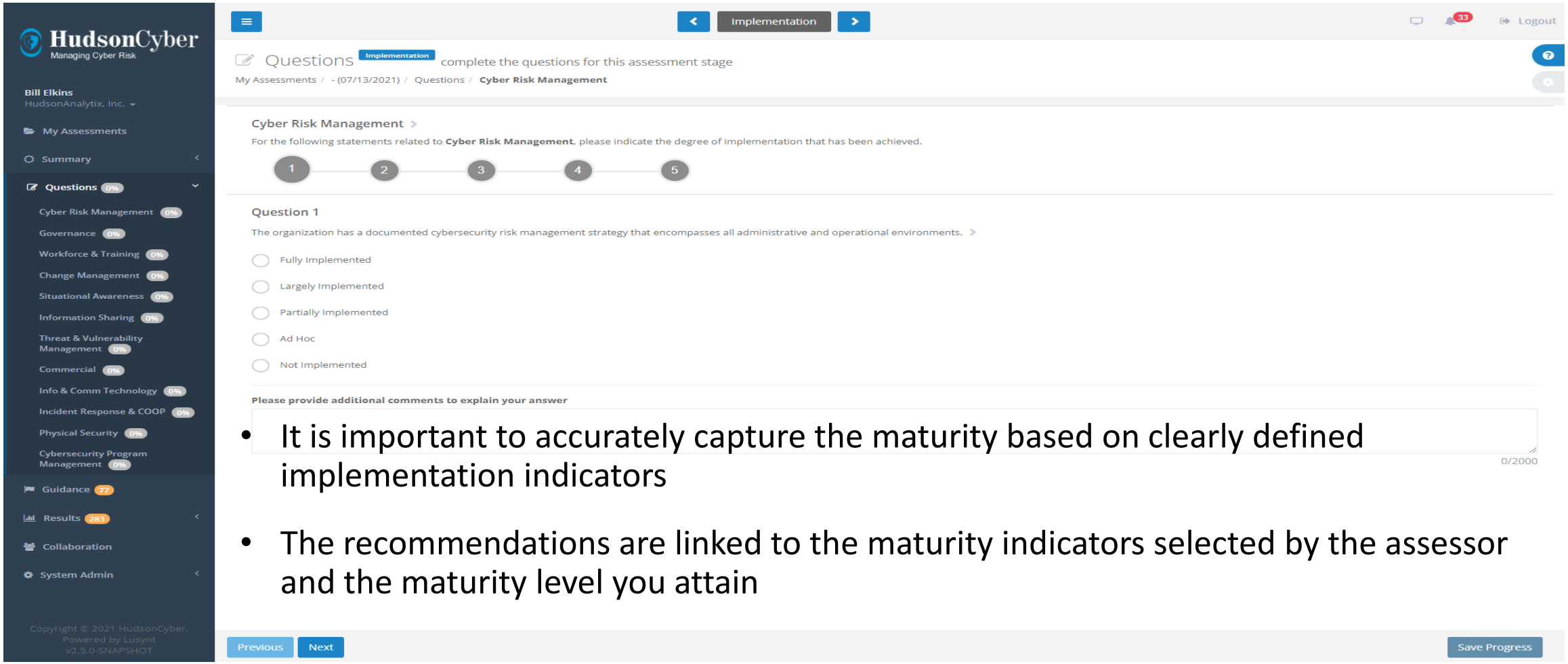
** The assumption that the team is prepared for the self-assessment; the level of detail will also impact the time.

Assessments are Assigned to Individual Users



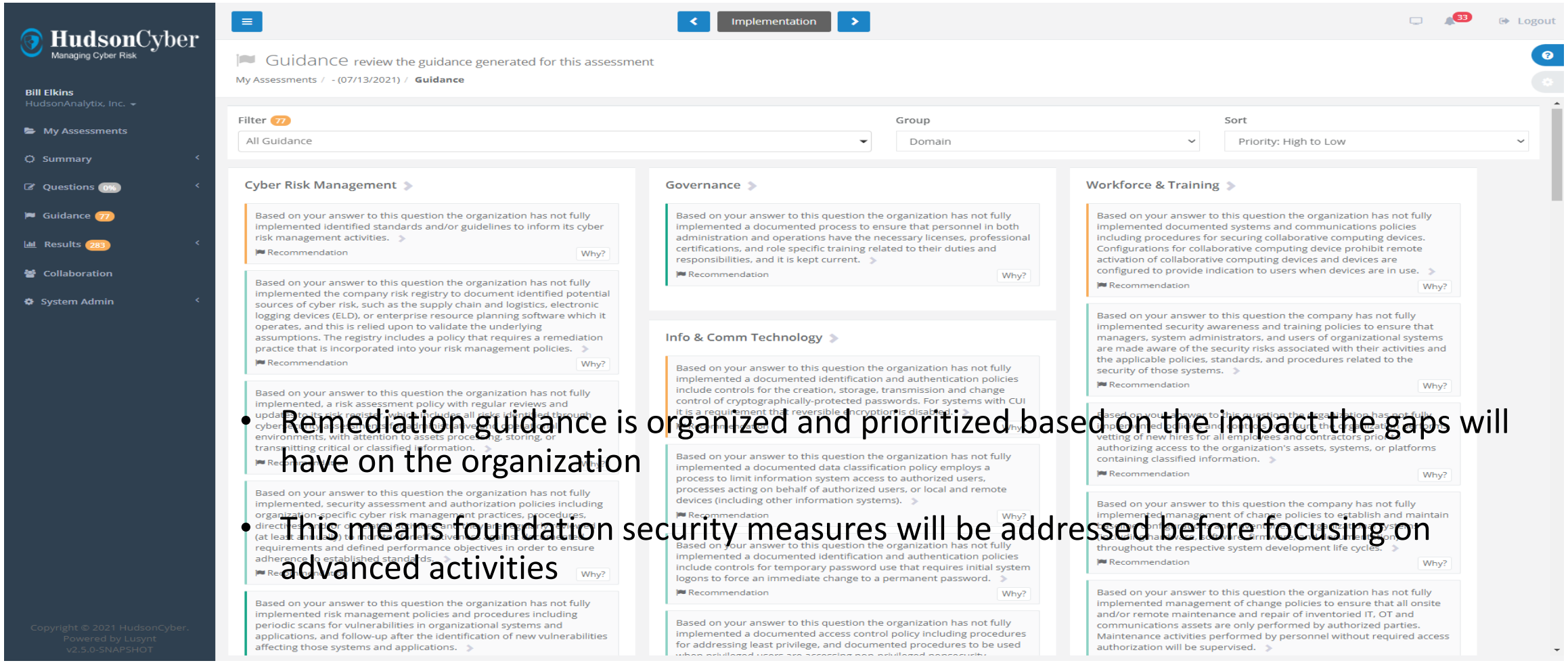
- Secure access to assessments is managed on both an individual and role basis
- Assessment progress and guidance are presented for all assessments
- Users can participate in more than one assessment

Assessment Maturity Questions by Domain



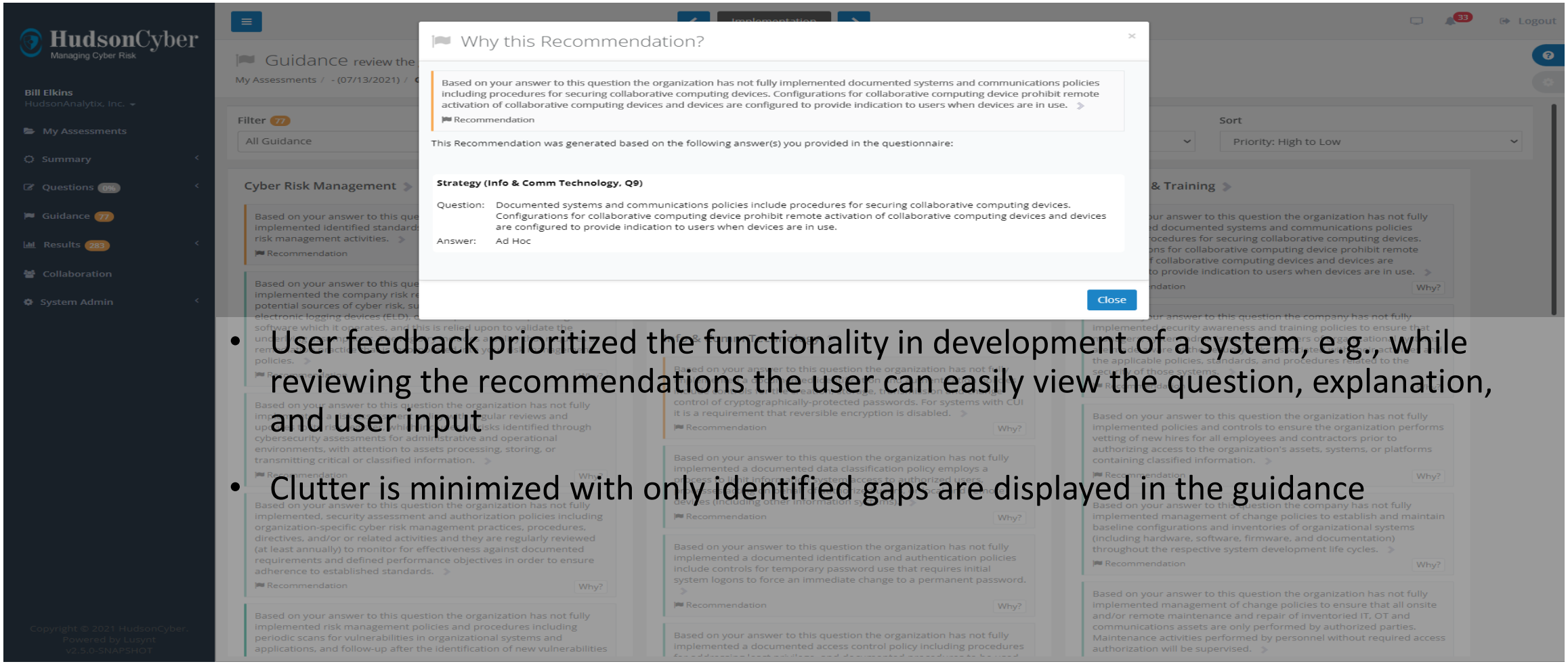
- It is important to accurately capture the maturity based on clearly defined implementation indicators
- The recommendations are linked to the maturity indicators selected by the assessor and the maturity level you attain

Guidance Addresses Identified Gaps



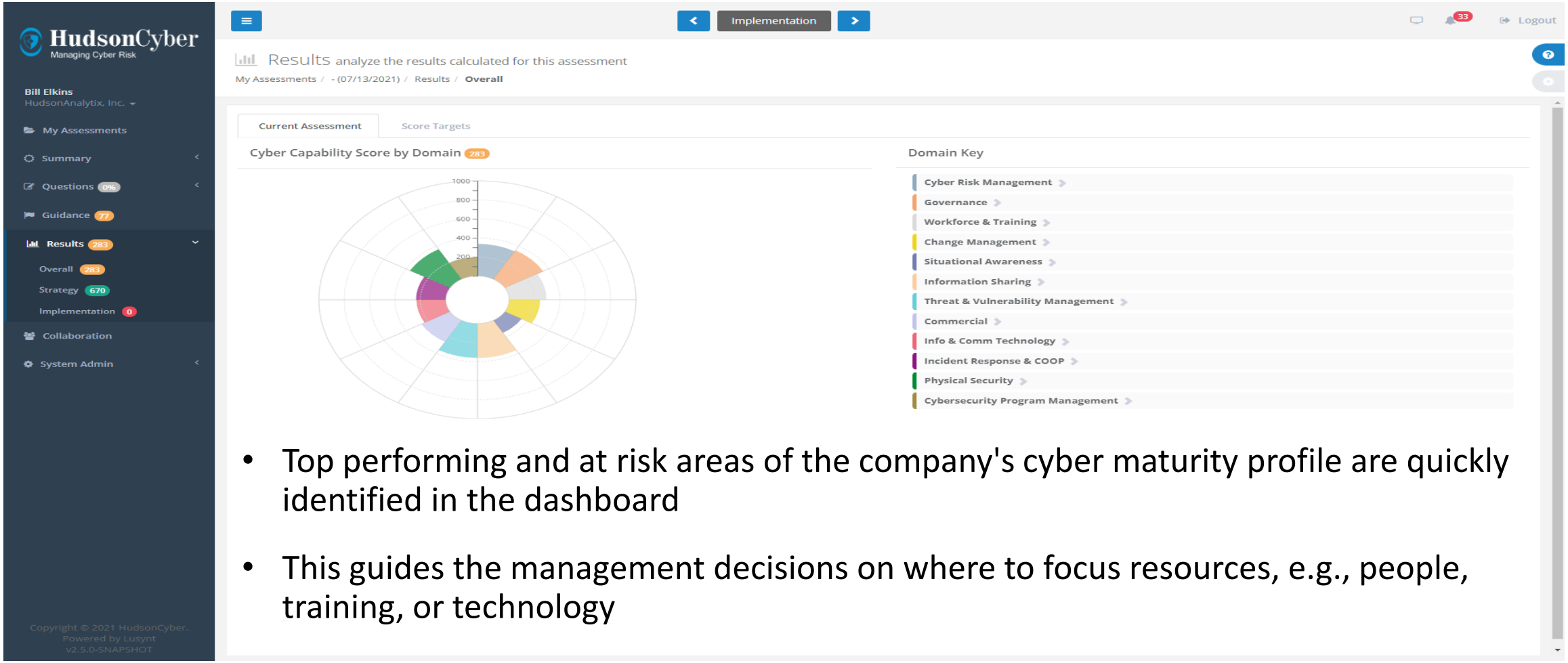
- Remediation guidance is organized and prioritized based on the impact the gaps will have on the organization
- This means foundation security measures will be addressed before focusing on advanced activities

Guidance Includes Clear Links to the Questions



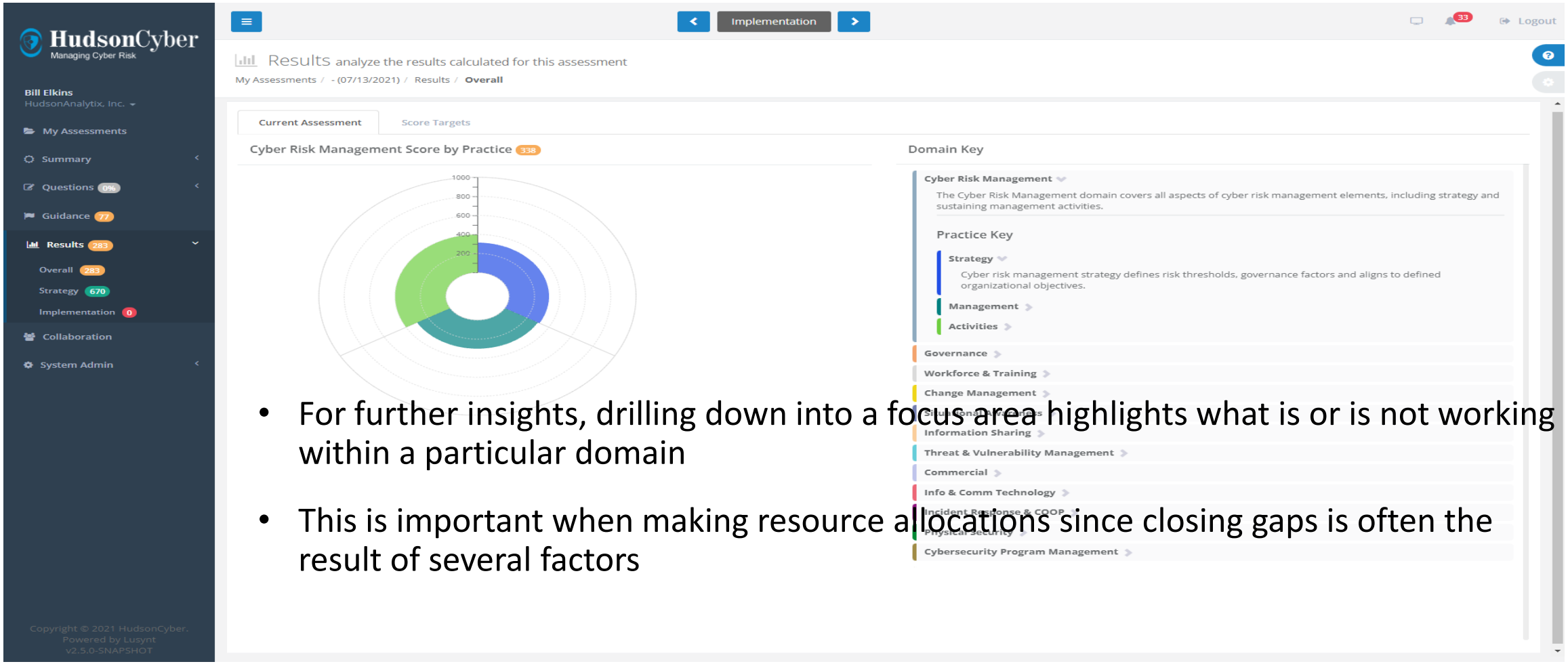
- User feedback prioritized the functionality in development of a system, e.g., while reviewing the recommendations the user can easily view the question, explanation, and user input
- Clutter is minimized with only identified gaps are displayed in the guidance

Cyber Capability Easily Compared by Domain



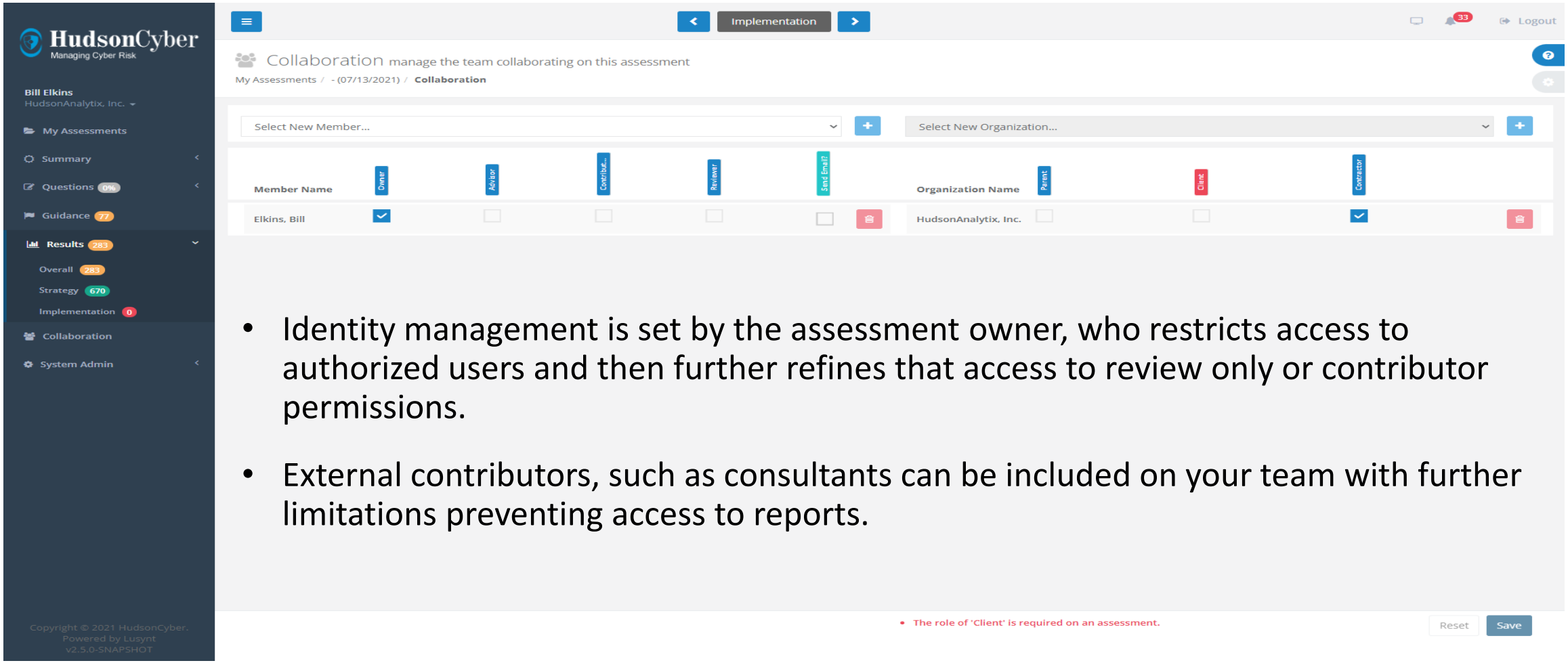
- Top performing and at risk areas of the company's cyber maturity profile are quickly identified in the dashboard
- This guides the management decisions on where to focus resources, e.g., people, training, or technology

Drill Down to Expose Influential Contributing Factors



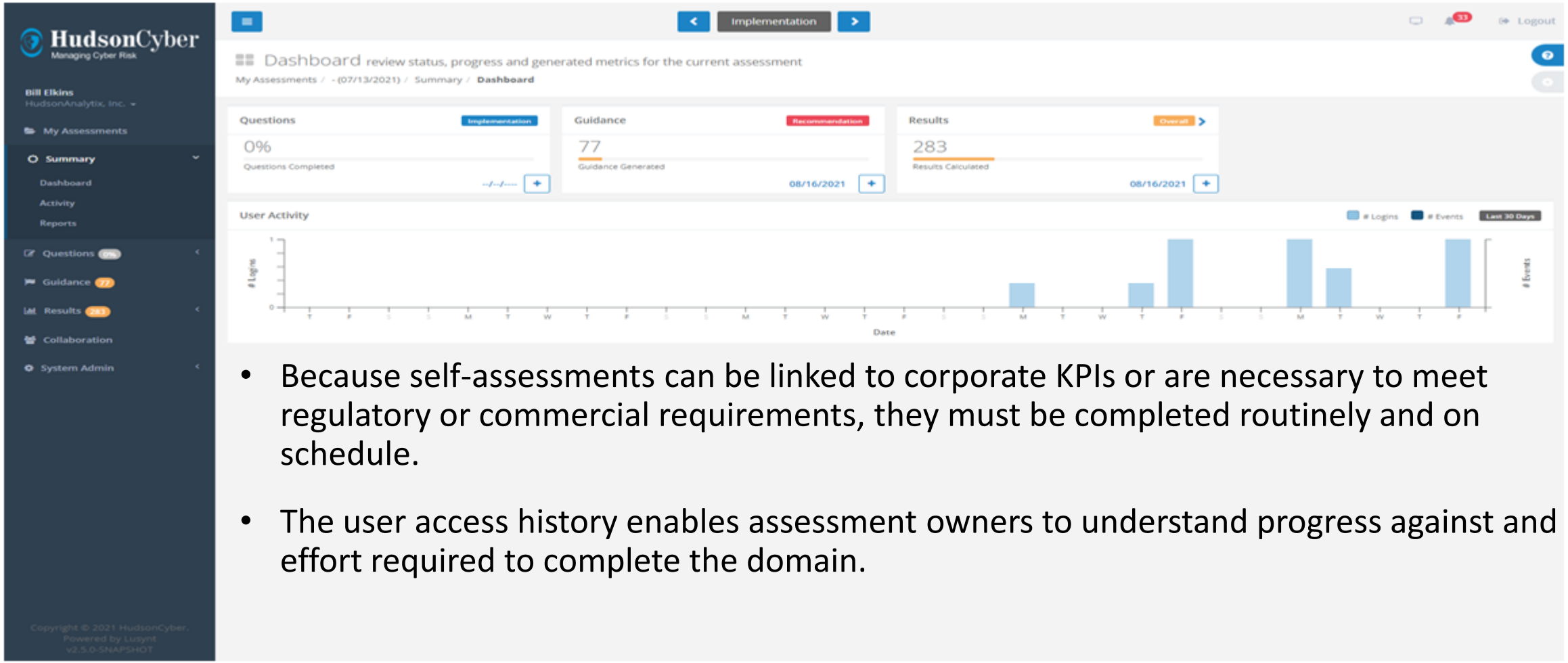
- For further insights, drilling down into a focus area highlights what is or is not working within a particular domain
- This is important when making resource allocations since closing gaps is often the result of several factors

Role Specific Security Access Controls



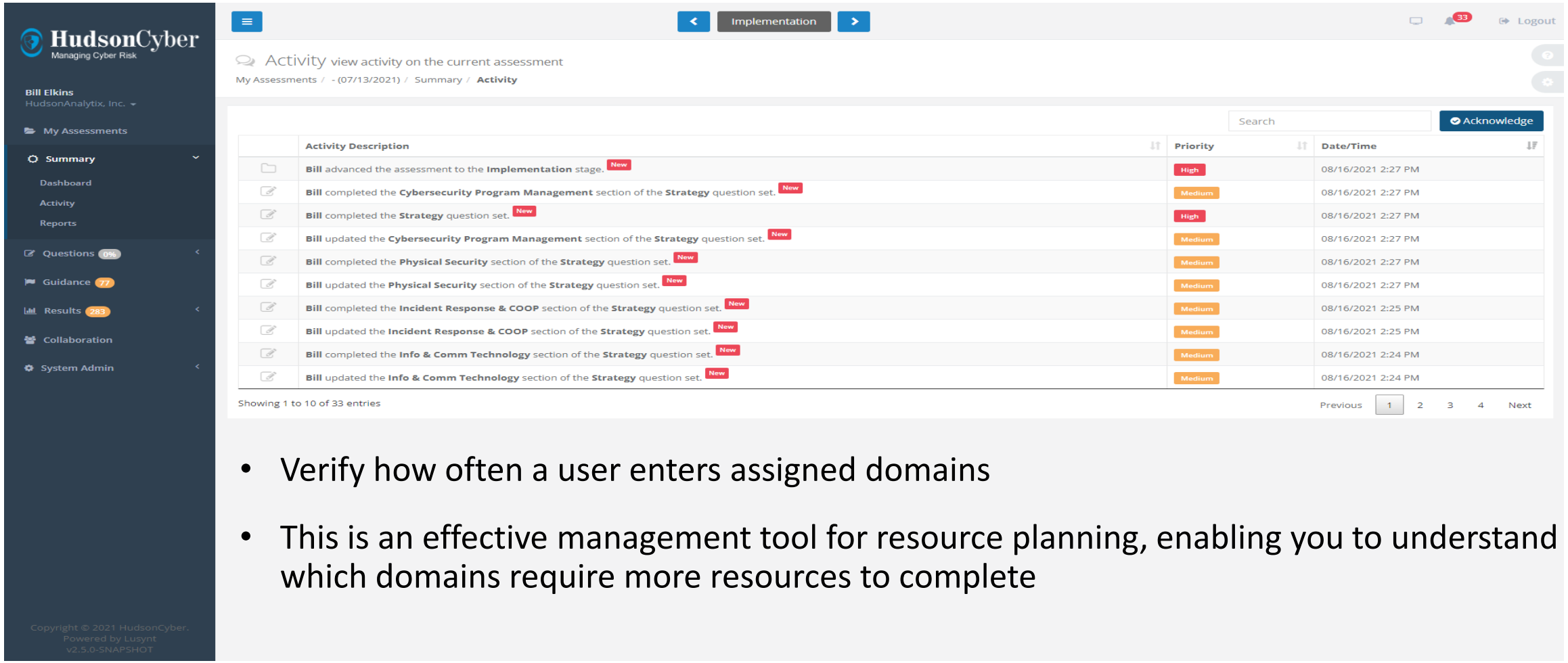
- Identity management is set by the assessment owner, who restricts access to authorized users and then further refines that access to review only or contributor permissions.
- External contributors, such as consultants can be included on your team with further limitations preventing access to reports.

Dashboard Shows User Activities on the Assessment



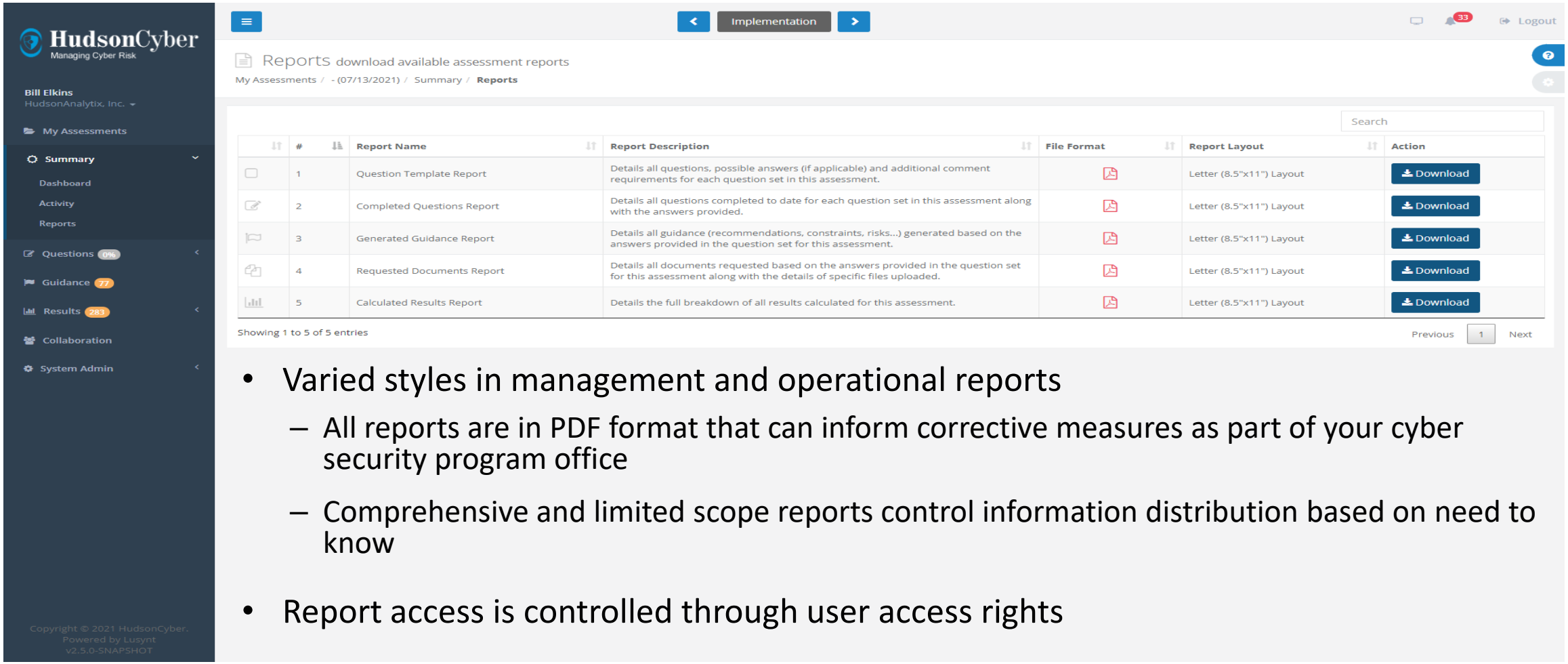
- Because self-assessments can be linked to corporate KPIs or are necessary to meet regulatory or commercial requirements, they must be completed routinely and on schedule.
- The user access history enables assessment owners to understand progress against and effort required to complete the domain.

Detailed Break Down for User Activity and Actions



- Verify how often a user enters assigned domains
- This is an effective management tool for resource planning, enabling you to understand which domains require more resources to complete

Functionally Targeted Management Reports



- Varied styles in management and operational reports
  - All reports are in PDF format that can inform corrective measures as part of your cyber security program office
  - Comprehensive and limited scope reports control information distribution based on need to know
- Report access is controlled through user access rights

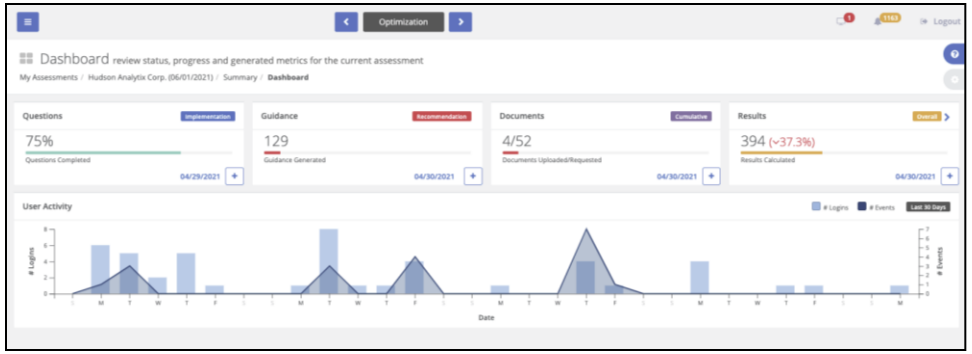
Applying Best Practices for Cyber Risk Management

- Incorporate cyber risk management into governance practices
  - Safety and security policies and practices
  - Personnel training and appraisal
  - Management of change
  - Auditing
- Performing continuous assessments against accepted standards
  - Assessments encompass NIST, CMMC, CTPAT, and NHTSA controls
  - Self-assessments reflect cyber maturity not a compliance checklist
- Incident preparedness, response and recovery
  - Company policies and procedures should reinforce best practices, and leverage all internal and external resources to prepare for, respond to, and recover from cyber events.
  - Just as cyber risks continually evolve the identification of cyber risks is continuous.

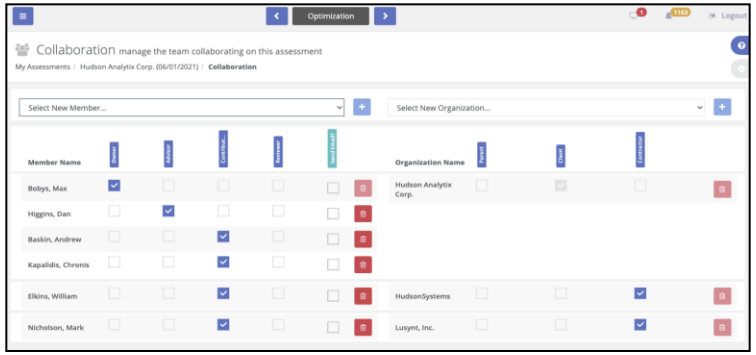
CYMETRICS Benefits

- Self-assessments can be performed at your convenience
- Clearly identifies gaps, and generates a maturity score to track efforts to close gaps
- Generates gap remediation tasks, with specific recommendations
- Manage multiple divisions from single solution
- Artifact upload for each question to organize documentation
- PDF reports include gaps, risks, and progress to meeting your cyber goals
- CYMETRICS is the most cost effective means of governing your cybersecurity initiative and ongoing management tasks

Manage Your Cybersecurity Efforts



Home Dashboard offers easy access to key data fields: scoring, recommendations, documentation and analysis inputs.

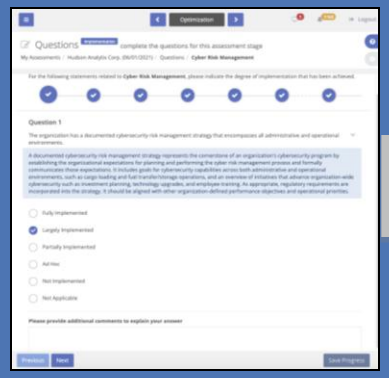


Drive Collaboration

Setup and Organize Virtual Teams

Assess

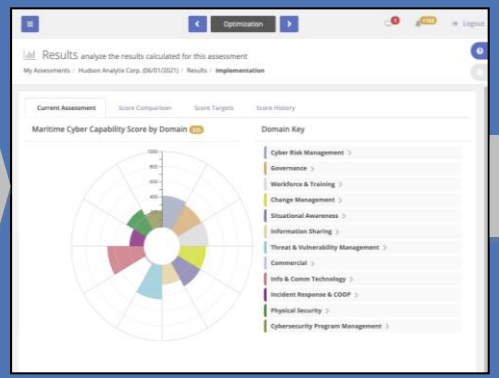
Capabilities



Assessment questions are dynamically generated and include detailed help text.

Pinpoint

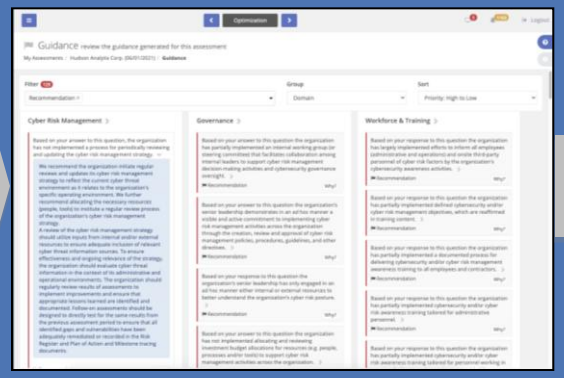
Gaps and Vulnerabilities



Scores are generated by practice area, functional domain and maturity level. Drill-down options allow for rapid review and analysis.

Identify

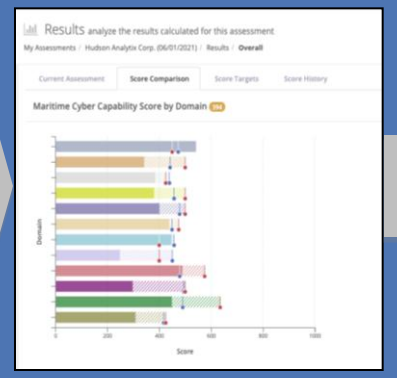
Solutions and Resource Options



Actionable Recommendations can be filtered by functional area, prioritized and organized by functional domain.

Benchmark

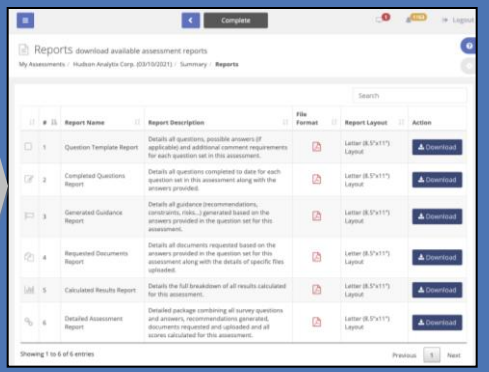
And Monitor Progress



Real Time Benchmarking monitors internal progress and tracks performance against industry peers.

Demonstrate

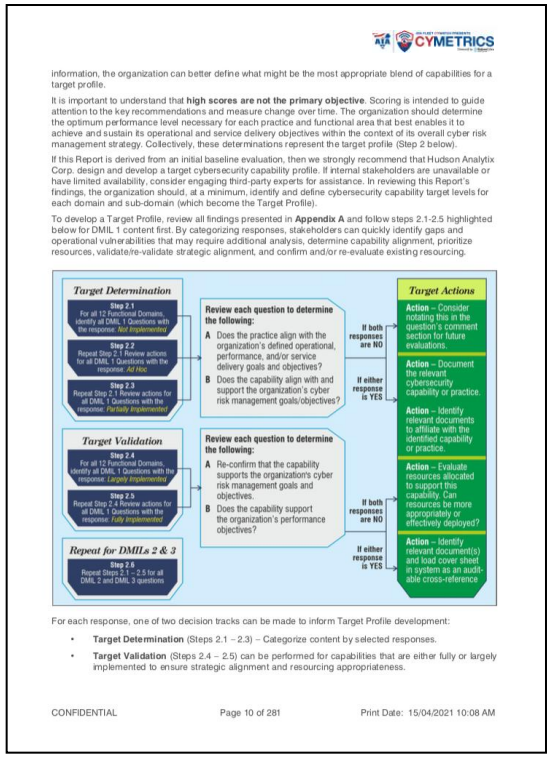
Compliance & Standard of Care



Reports are available for download on demand.

Sustainable Cybersecurity Program Management

Collaborate
via Hands-on Engagement



information, the organization can better define what might be the most appropriate blend of capabilities for a target profile.

It is important to understand that **high scores are not the primary objective**. Scoring is intended to guide attention to the key recommendations and measure change over time. The organization should determine the optimum performance level necessary for each practice and functional area that best enables it to achieve and sustain its operational and service delivery objectives within the context of its overall cyber risk management strategy. Collectively, these determinations represent the target profile (Step 2 below).

If this Report is derived from an initial baseline evaluation, then we strongly recommend that Hudson Analytix Corp. design and develop a target cybersecurity capability profile. If internal stakeholders are unavailable or have limited availability, consider engaging third-party experts for assistance. In reviewing this Report's findings, the organization should, at a minimum, identify and define cybersecurity capability target levels for each domain and sub-domain (which become the Target Profile).

To develop a Target Profile, review all findings presented in **Appendix A** and follow steps 2.1-2.5 highlighted below for DMIL 1 content first. By categorizing responses, stakeholders can quickly identify gaps and operational vulnerabilities that may require additional analysis, determine capability alignment, prioritize resources, validate/re-validate strategic alignment, and confirm and/or re-evaluate existing resourcing.

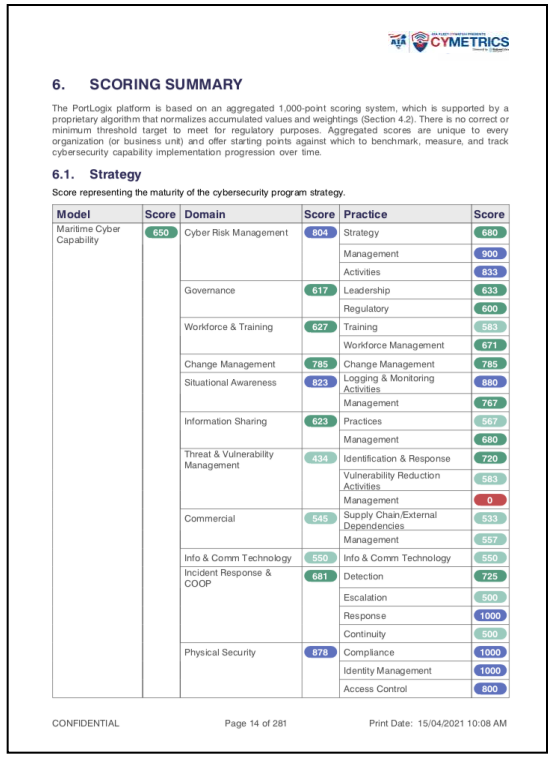
For each response, one of two decision tracks can be made to inform Target Profile development:

- **Target Determination** (Steps 2.1 – 2.3) – Categorize content by selected responses.
- **Target Validation** (Steps 2.4 – 2.5) can be performed for capabilities that are either fully or largely implemented to ensure strategic alignment and resourcing appropriateness.

CONFIDENTIAL Page 10 of 281 Print Date: 15/04/2021 10:08 AM

Step-by-step guidance assists users in developing realistic target profiles based on hands-on analysis.

Focus
Resources on Actual Needs



6. SCORING SUMMARY

The PortLogix platform is based on an aggregated 1,000-point scoring system, which is supported by a proprietary algorithm that normalizes accumulated values and weightings (Section 4.2). There is no correct or minimum threshold target to meet for regulatory purposes. Aggregated scores are unique to every organization (or business unit) and offer starting points against which to benchmark, measure, and track cybersecurity capability implementation progression over time.

6.1. Strategy

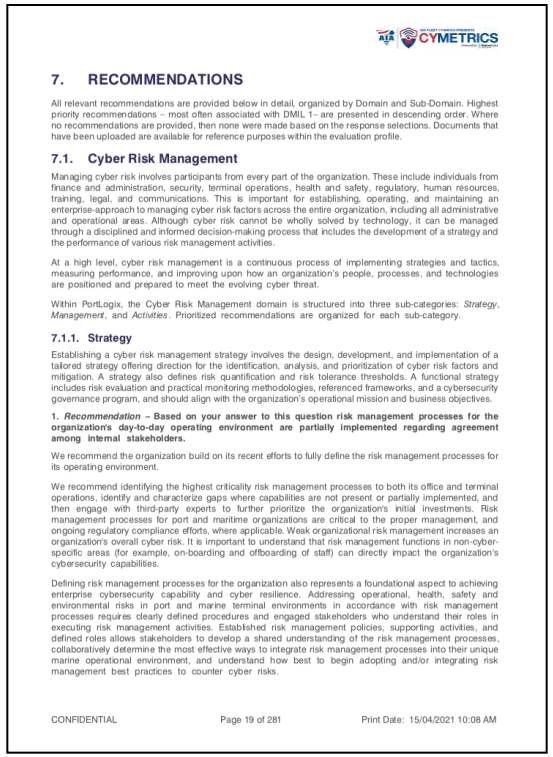
Score representing the maturity of the cybersecurity program strategy.

Model	Score	Domain	Score	Practice	Score
Maritime Cyber Capability	650	Cyber Risk Management	804	Strategy	680
				Management	900
				Activities	833
		Governance	617	Leadership	633
				Regulatory	600
		Workforce & Training	627	Training	583
				Workforce Management	671
		Change Management	785	Change Management	785
		Situational Awareness	823	Logging & Monitoring	880
				Management	767
		Information Sharing	623	Practices	567
				Management	680
		Threat & Vulnerability Management	434	Identification & Response	720
				Vulnerability Reduction Activities	583
				Management	0
		Commercial	545	Supply Chain/External Dependencies	533
				Management	557
		Info & Comm Technology	550	Info & Comm Technology	550
		Incident Response & COOP	681	Detection	725
				Escalation	500
				Response	1000
				Continuity	500
		Physical Security	878	Compliance	1000
				Identity Management	1000
				Access Control	800

CONFIDENTIAL Page 14 of 281 Print Date: 15/04/2021 10:08 AM

Scoring enables rapid review and analysis to assist in the identification of capability gaps and vulnerabilities.

Save Money
By Investing Efficiently



7. RECOMMENDATIONS

All relevant recommendations are provided below in detail, organized by Domain and Sub-Domain. Highest priority recommendations – most often associated with DMIL 1– are presented in descending order. Where no recommendations are provided, then none were made based on the response selections. Documents that have been uploaded are available for reference purposes within the evaluation profile.

7.1. Cyber Risk Management

Managing cyber risk involves participants from every part of the organization. These include individuals from finance and administration, security, terminal operations, health and safety, regulatory, human resources, training, legal, and communications. This is important for establishing, operating, and maintaining an enterprise-approach to managing cyber risk factors across the entire organization, including all administrative and operational areas. Although cyber risk cannot be wholly solved by technology, it can be managed through a disciplined and informed decision-making process that includes the development of a strategy and the performance of various risk management activities.

At a high level, cyber risk management is a continuous process of implementing strategies and tactics, measuring performance, and improving upon how an organization's people, processes, and technologies are positioned and prepared to meet the evolving cyber threat.

Within PortLogix, the Cyber Risk Management domain is structured into three sub-categories: *Strategy*, *Management*, and *Activities*. Prioritized recommendations are organized for each sub-category.

7.1.1. Strategy

Establishing a cyber risk management strategy involves the design, development, and implementation of a tailored strategy offering direction for the identification, analysis, and prioritization of cyber risk factors and mitigation. A strategy also defines risk quantification and risk tolerance thresholds. A functional strategy includes risk evaluation and practical monitoring methodologies, referenced frameworks, and a cybersecurity governance program, and should align with the organization's operational mission and business objectives.

1. ***Recommendation*** **– Based on your answer to this question risk management processes for the organization's day-to-day operating environment are partially implemented regarding agreement among internal stakeholders.**

We recommend the organization build on its recent efforts to fully define the risk management processes for its operating environment.

We recommend identifying the highest criticality risk management processes to both its office and terminal operations, identify and characterize gaps where capabilities are not present or partially implemented, and then engage with third-party experts to further prioritize the organization's initial investments. Risk management processes for port and maritime organizations are critical to the proper management, and ongoing regulatory compliance efforts, where applicable. Weak organizational risk management increases an organization's overall cyber risk. It is important to understand that risk management functions in non-cyber-specific areas (for example, on-boarding and offboarding of staff) can directly impact the organization's cybersecurity capabilities.

Defining risk management processes for the organization also represents a foundational aspect to achieving enterprise cybersecurity capability and cyber resilience. Addressing operational, health, safety and environmental risks in port and marine terminal environments in accordance with risk management processes requires clearly defined procedures and engaged stakeholders who understand their roles in executing risk management activities. Established risk management policies, supporting activities, and defined roles allows stakeholders to develop a shared understanding of the risk management processes, collaboratively determine the most effective ways to integrate risk management processes into their unique marine operational environment, and understand how best to begin adopting and/or integrating risk management best practices to counter cyber risks.

CONFIDENTIAL Page 19 of 281 Print Date: 15/04/2021 10:08 AM

Recommendations are organized by functional domain and prioritized.

Conclusion

- As with most things, prevention is better than a cure, gaining a solid understanding of your organizations cyber maturity is a critical management task.
- It’s not possible to eradicate cyber security risks, so organizations need to create a layered security system where vulnerabilities can be identified in multiple ways. An organization's biggest weakness is often personnel, so cyber awareness training is vital.
- Many attacks stem from technical vulnerabilities, so organizations should also implement controls and conduct regular penetration tests to assess the effectiveness of their systems’ security.
- Leadership should make identification, cyber program management, and operational management of cyber risk a organizational imitative that engages personnel at all levels.

Contact Us for Additional Information

- About CYMETRICS
  - Visit https://cymetrics.ha-cyberlogix.com
  - Use the Contact Us form to request a follow-up call
  - Email cymetrics@hudsoncyber.com
- About consulting assistance with your cybersecurity initiative
  - Email cymetrics@hudsoncyber.com

For Additional Information

HudsonCyber
Managing Cyber Risk

1800 Chapel Avenue West
Suite 360
Cheery Hill, NJ 08002

William J. Elkins
Chief Technology Officer

Office: +1.856.342.7500
Mobile: +1.856.308.6347
Email: william.elkins@hudsoncyber.com