



Driving Your Cybersecurity Program An Overview of CYMETRICS

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

Copyright © 2021 HudsonCyber. Powered by Lusynt v2.5.0-SNAPSHOT

- 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

The screenshot displays the HudsonCyber assessment interface. The left sidebar shows the user 'Bill Elkins' and a navigation menu with categories like 'My Assessments', 'Summary', 'Questions' (0%), 'Guidance' (77%), 'Results' (283), 'Collaboration', and 'System Admin'. The main content area is titled 'Implementation' and shows 'Questions' for the 'Cyber Risk Management' domain. A progress indicator shows five steps, with the first step selected. The question asks for the degree of implementation for a statement: 'The organization has a documented cybersecurity risk management strategy that encompasses all administrative and operational environments.' The options are: Fully Implemented, Largely Implemented, Partially Implemented, Ad Hoc, and Not Implemented. A text box for additional comments is present, with a character count of 0/2000. The interface includes navigation buttons for 'Previous', 'Next', and 'Save Progress'.

Implementation

Questions **Implementation** complete the questions for this assessment stage

My Assessments / - (07/13/2021) / Questions / **Cyber Risk Management**

Cyber Risk Management

For the following statements related to **Cyber Risk Management**, please indicate the degree of implementation that has been achieved.

1 2 3 4 5

Question 1

The organization has a documented cybersecurity risk management strategy that encompasses all administrative and operational environments. >

Fully Implemented

Largely Implemented

Partially Implemented

Ad Hoc

Not Implemented

Please provide additional comments to explain your answer

- 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

0/2000

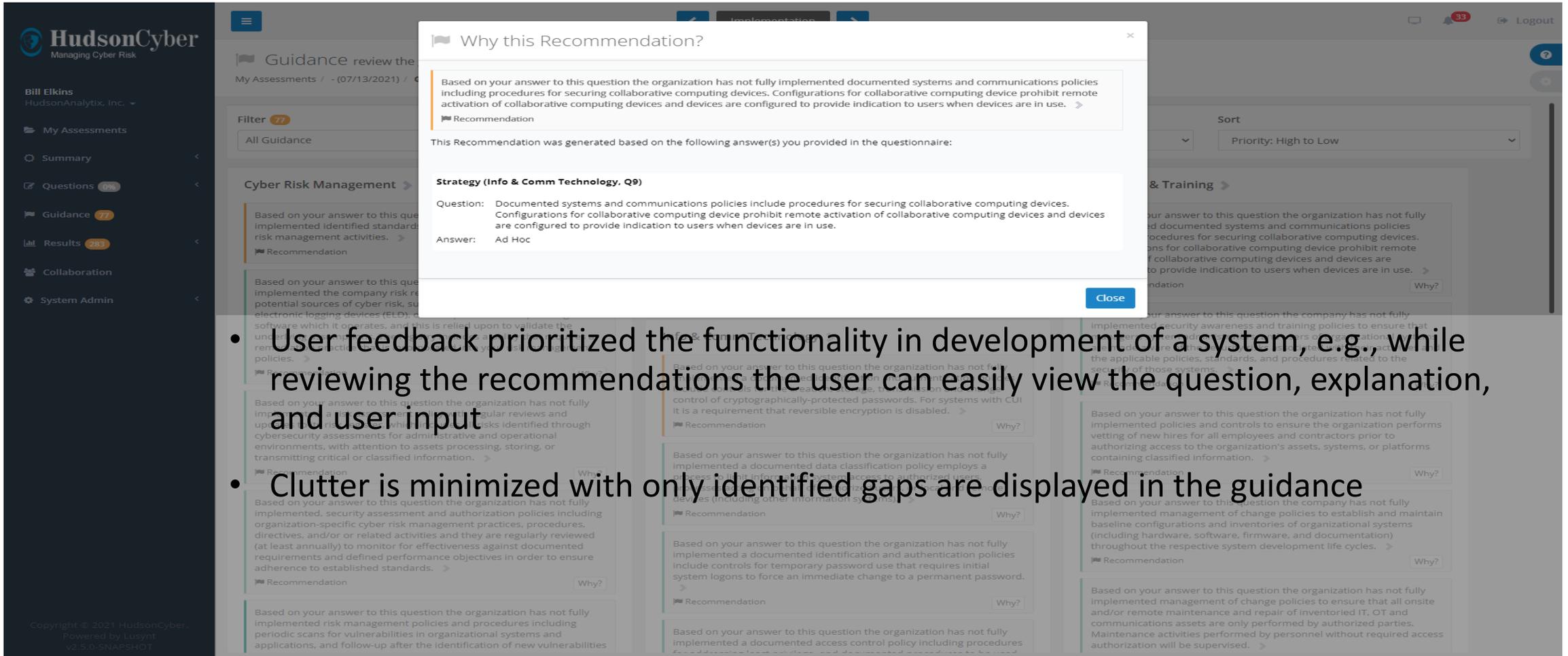
Previous Next Save Progress

Guidance Addresses Identified Gaps

The screenshot displays the HudsonCyber 'Guidance' interface. The top navigation bar includes 'Implementation' and 'Logout'. The main content area is titled 'Guidance review the guidance generated for this assessment' and shows 'My Assessments / - (07/13/2021) / Guidance'. A filter bar indicates 77 items, with a 'Group' dropdown set to 'Domain' and a 'Sort' dropdown set to 'Priority: High to Low'. The interface is divided into three columns: 'Cyber Risk Management', 'Governance', and 'Workforce & Training'. Each column contains several recommendation cards, each starting with a 'Based on your answer to this question...' statement and followed by a 'Recommendation' and a 'Why?' link. The recommendations cover topics such as risk management standards, documented processes for personnel, security awareness training, data classification policies, and change management procedures.

- 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



The screenshot shows the HudsonCyber interface with a modal window titled "Why this Recommendation?". The modal contains the following text:

Based on your answer to this question the organization has not fully implemented documented systems and communications policies including procedures for securing collaborative computing devices. Configurations for collaborative computing device prohibit remote activation of collaborative computing devices and devices are configured to provide indication to users when devices are in use. >

Recommendation

This Recommendation was generated based on the following answer(s) you provided in the questionnaire:

Strategy (Info & Comm Technology, Q9)

Question: Documented systems and communications policies include procedures for securing collaborative computing devices. Configurations for collaborative computing device prohibit remote activation of collaborative computing devices and devices are configured to provide indication to users when devices are in use.

Answer: Ad Hoc

Close

- 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

The screenshot displays the HudsonCyber dashboard for user Bill Elkins. The main content area shows the 'Results' section for an assessment conducted on 07/13/2021, with an overall score of 283. A radar chart titled 'Cyber Capability Score by Domain' visualizes the scores across ten domains. The 'Domain Key' on the right lists these domains with corresponding color-coded arrows pointing to the chart segments.

Domain	Score (Approximate)
Cyber Risk Management	200
Governance	150
Workforce & Training	100
Change Management	100
Situational Awareness	100
Information Sharing	100
Threat & Vulnerability Management	100
Commercial	100
Info & Comm Technology	100
Incident Response & COOP	100
Physical Security	100
Cybersecurity Program Management	100

- 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

The screenshot displays the HudsonCyber assessment results interface. The left sidebar shows the user 'Bill Elkins' and navigation options like 'My Assessments', 'Summary', 'Questions', 'Guidance', 'Results', 'Overall', 'Strategy', 'Implementation', 'Collaboration', and 'System Admin'. The main content area is titled 'Results' and shows 'Cyber Risk Management Score by Practice' with a score of 338. A radar chart visualizes the score across various domains. A 'Domain Key' section on the right provides a detailed breakdown of the 'Cyber Risk Management' domain, including a 'Practice Key' with sub-sections for Strategy, Management, and Activities, and a list of other domains like Governance, Workforce & Training, Change Management, etc.

- 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

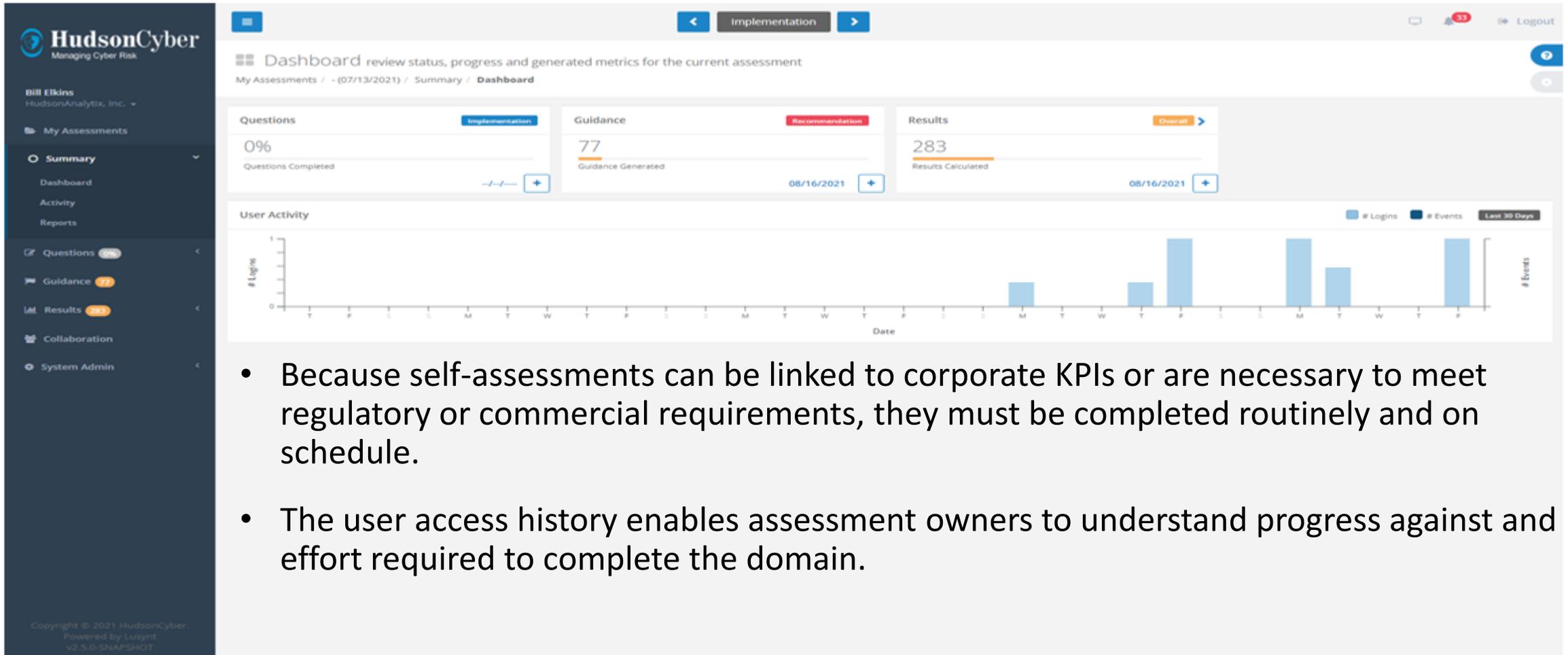
Role Specific Security Access Controls

The screenshot displays the HudsonCyber Collaboration interface. The top navigation bar includes a menu icon, a breadcrumb trail for 'Implementation', and a 'Logout' button. The main header shows 'Collaboration manage the team collaborating on this assessment' and the current assessment path: 'My Assessments / - (07/13/2021) / Collaboration'. Below this, there are two dropdown menus for 'Select New Member...' and 'Select New Organization...'. The main content area features a table with columns for 'Member Name' and 'Organization Name', and rows for 'Elkins, Bill' and 'HudsonAnalytix, Inc.'. Each cell in the table contains a role selector dropdown and a checkbox. The roles available are Owner, Advisor, Contributor, Reviewer, and Client. The 'Client' role is highlighted in red. At the bottom right, there are 'Reset' and 'Save' buttons. A red note at the bottom center states: '• The role of 'Client' is required on an assessment.'

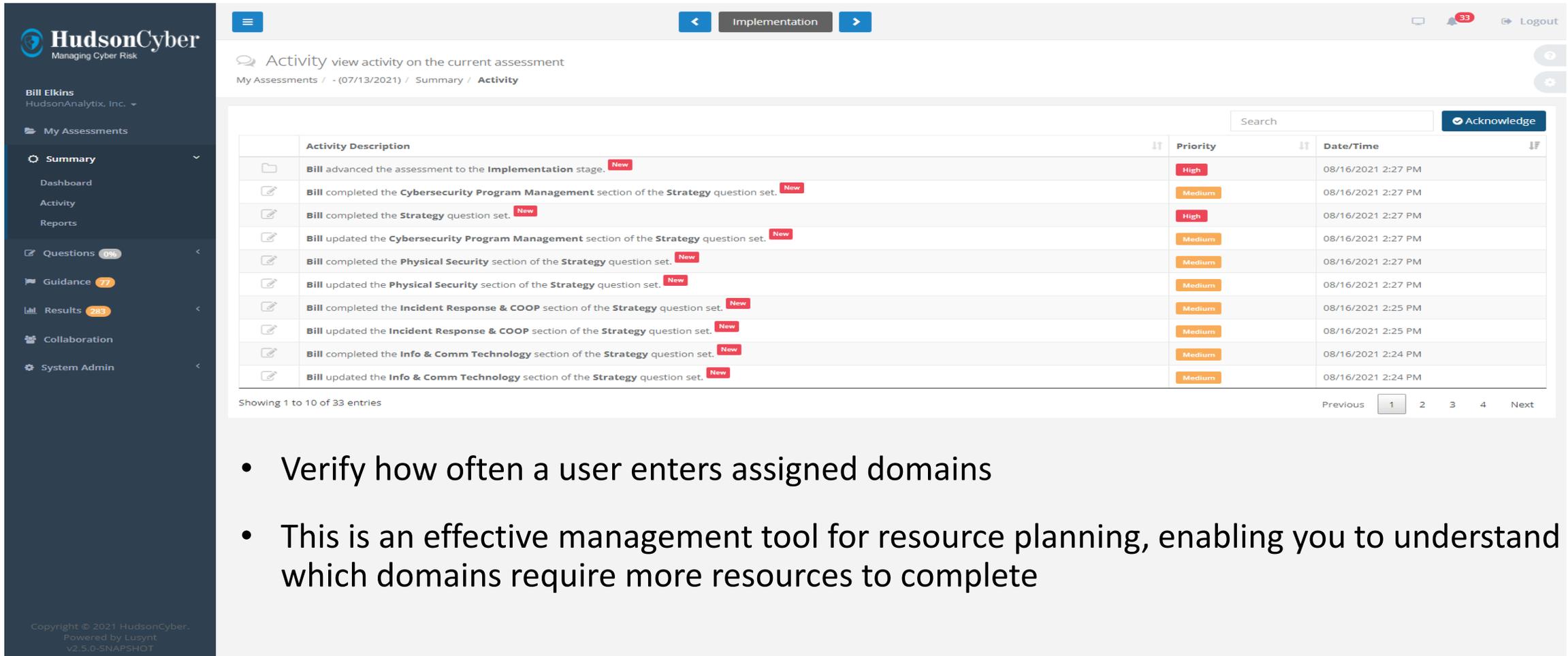
Member Name	Owner	Advisor	Contributor	Reviewer	Client	Organization Name	Parent	Client	Contributor
Elkins, Bill	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HudsonAnalytix, Inc.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- 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



Detailed Break Down for User Activity and Actions



The screenshot displays the HudsonCyber interface for the 'Implementation' stage. The left sidebar shows the user 'Bill Elkins' and navigation options like 'My Assessments', 'Summary', 'Dashboard', 'Activity', 'Reports', 'Questions (0%)', 'Guidance (77)', 'Results (283)', 'Collaboration', and 'System Admin'. The main content area shows a list of activities with columns for 'Activity Description', 'Priority', and 'Date/Time'. The activities include actions like 'Bill advanced the assessment to the Implementation stage', 'Bill completed the Cybersecurity Program Management section of the Strategy question set', and 'Bill updated the Physical Security section of the Strategy question set'. The priority levels range from High to Medium. A search bar and an 'Acknowledge' button are also visible.

Activity Description	Priority	Date/Time
Bill advanced the assessment to the Implementation stage. New	High	08/16/2021 2:27 PM
Bill completed the Cybersecurity Program Management section of the Strategy question set. New	Medium	08/16/2021 2:27 PM
Bill completed the Strategy question set. New	High	08/16/2021 2:27 PM
Bill updated the Cybersecurity Program Management section of the Strategy question set. New	Medium	08/16/2021 2:27 PM
Bill completed the Physical Security section of the Strategy question set. New	Medium	08/16/2021 2:27 PM
Bill updated the Physical Security section of the Strategy question set. New	Medium	08/16/2021 2:27 PM
Bill completed the Incident Response & COOP section of the Strategy question set. New	Medium	08/16/2021 2:25 PM
Bill updated the Incident Response & COOP section of the Strategy question set. New	Medium	08/16/2021 2:25 PM
Bill completed the Info & Comm Technology section of the Strategy question set. New	Medium	08/16/2021 2:24 PM
Bill updated the Info & Comm Technology section of the Strategy question set. New	Medium	08/16/2021 2:24 PM

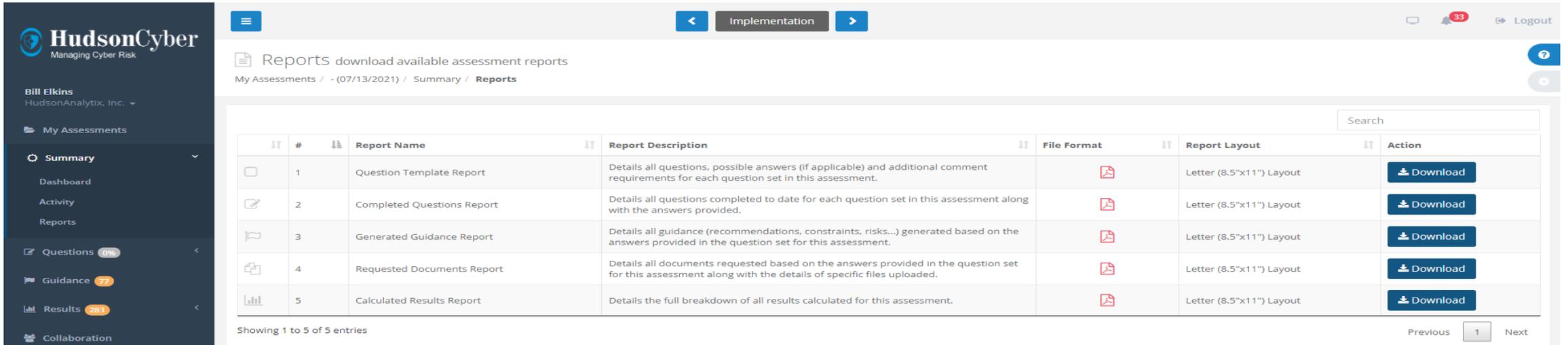
Showing 1 to 10 of 33 entries

Previous 1 2 3 4 Next

- 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

Copyright © 2021 HudsonCyber. Powered by Lusynt v2.5.0-SNAPSHOT

Functionally Targeted Management Reports



The screenshot displays the HudsonCyber Reports interface. The left sidebar shows the user's profile (Bill Elkins, HudsonAnalytix, Inc.) and navigation options (My Assessments, Summary, Dashboard, Activity, Reports, Questions, Guidance, Results, Collaboration, System Admin). The main content area shows a list of reports under the 'Implementation' tab. The table below details the reports:

#	Report Name	Report Description	File Format	Report Layout	Action
1	Question Template Report	Details all questions, possible answers (if applicable) and additional comment requirements for each question set in this assessment.	PDF	Letter (8.5"x11") Layout	Download
2	Completed Questions Report	Details all questions completed to date for each question set in this assessment along with the answers provided.	PDF	Letter (8.5"x11") Layout	Download
3	Generated Guidance Report	Details all guidance (recommendations, constraints, risks...) generated based on the answers provided in the question set for this assessment.	PDF	Letter (8.5"x11") Layout	Download
4	Requested Documents Report	Details all documents requested based on the answers provided in the question set for this assessment along with the details of specific files uploaded.	PDF	Letter (8.5"x11") Layout	Download
5	Calculated Results Report	Details the full breakdown of all results calculated for this assessment.	PDF	Letter (8.5"x11") Layout	Download

Showing 1 to 5 of 5 entries

- 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

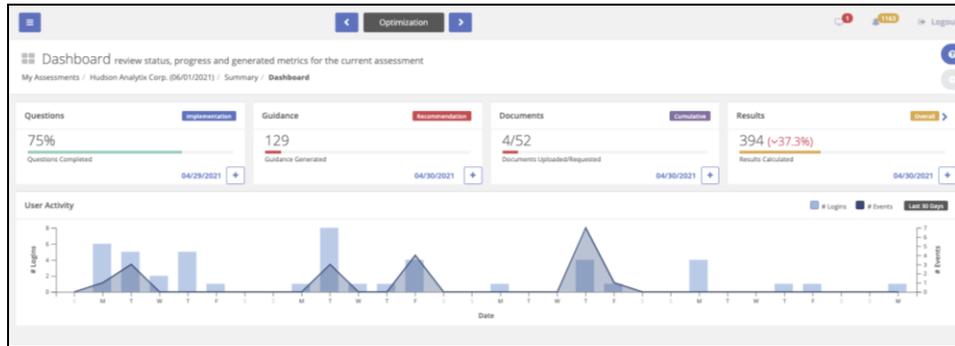
Applying Best Practices for Cyber Risk Management

- 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.

Member Name	Organization Name
Botly, Max	Hudson Analytic Corp.
Higgins, Dan	Hudson Analytic Corp.
Baskin, Andrew	Hudson Analytic Corp.
Kapalidis, Chronis	Hudson Analytic Corp.
Elkins, William	HudsonSystems
Nicholson, Mark	Luyinc, Inc.

Drive Collaboration
Setup and Organize Virtual Teams

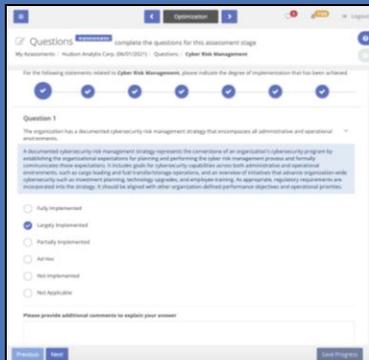
Assess Capabilities

Pinpoint Gaps and Vulnerabilities

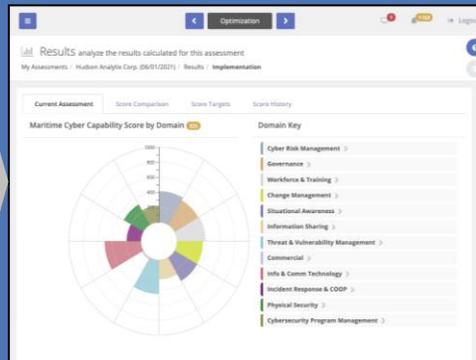
Identify Solutions and Resource Options

Benchmark And Monitor Progress

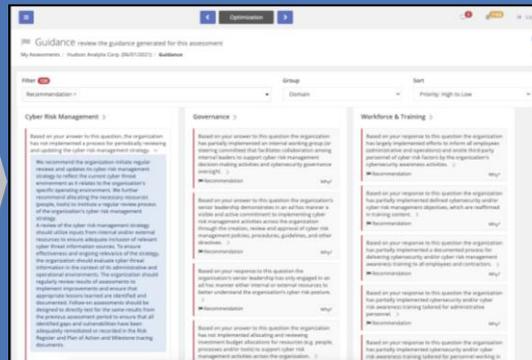
Demonstrate Compliance & Standard of Care



Assessment questions are dynamically generated and include detailed help text.



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



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



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

#	Report Name	Report Description	File Format	Report Layout	Action
1	Question Template Report	Details of all questions, possible answers (if applicable) and additional comment requirements for each question set in this assessment.	Letter (8.5x11) Layout	Download	
2	Completed Questions Report	Details of all questions completed to date for each question set in this assessment along with the answers provided.	Letter (8.5x11) Layout	Download	
3	Generated Guidance Report	Details of guidance recommendations, generated on this assessment based on the answers provided in the question set for this assessment along with the details of specific files applicable.	Letter (8.5x11) Layout	Download	
4	Requested Documents Report	Details of all documents requested based on the answers provided in the question set for this assessment along with the details of specific files applicable.	Letter (8.5x11) Layout	Download	
5	Calculated Results Report	Details of the full breakdown of all results calculated for this assessment.	Letter (8.5x11) Layout	Download	
6	Detailed Assessment Report	Detailed package combining all survey questions and answers, recommendations generated, documents requested and uploaded and all scores calculated for this assessment.	Letter (8.5x11) Layout	Download	

Reports are available for download on demand.

Sustainable Cybersecurity Program Management

Collaborate
via Hands-on Engagement

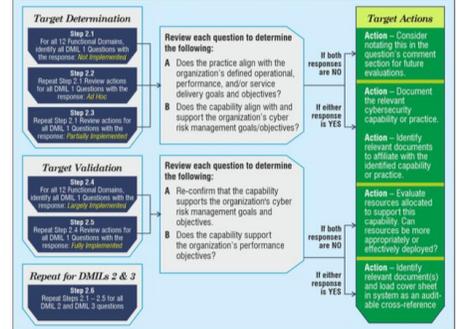


Information, the organization can better define what might be the most appropriate blend of capabilities for a target profile.

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 Analytic 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.



Target Determination

Step 2.1 For all 12 National Domains, identify at DMIL 1 Questions with the response: *Not Implemented*

Step 2.2 Repeat Step 2.1. Review actions for all DMIL 1 Questions with the response: *Not Implemented*

Step 2.3 Repeat Step 2.1. Review actions for all DMIL 1 Questions with the response: *Partially Implemented*

Target Validation

Step 2.4 For all 12 National Domains, identify at DMIL 1 Questions with the response: *Partially Implemented*

Step 2.5 Repeat Step 2.4. Review actions for all DMIL 1 Questions with the response: *Partially Implemented*

Step 2.6 Repeat Step 2.5. Review actions for all DMIL 2 and DMIL 3 questions

Review each question to determine the following:

A Does the practice align with the organization's defined operational, performance, and/or service delivery goals and objectives?

B Does the capability align with and support the organization's cyber risk management goals/objectives?

If both responses are NO

If either response is YES

Target Actions

Action - Consider noting this in the question's comment section for future evaluations.

Action - Document the relevant cybersecurity capability or practice.

Action - Identify relevant documents to align with the identified capability or practice.

Action - Evaluate resources allocated to support this capability. Are resources more appropriate or effective employed?

Action - Identify relevant document(s) and how covered them in system as an auditable cross-reference

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 assure 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	633
Governance				Leadership	633
				Regulatory	600
				Training	583
Workforce & Training				Workforce Management	671
				Change Management	785
Situational Awareness				Logging & Monitoring	880
				Activities	767
				Management	567
Information Sharing				Practices	680
				Management	720
				Identification & Response	583
Threat & Vulnerability Management				Vulnerability Reduction	0
				Activities	533
				Management	557
Commercial				Supply Chain/External Dependencies	557
				Management	550
				Info & Comm Technology	550
Incident Response & COOP				Detection	725
				Escalation	1000
				Response	500
Physical Security				Continuity	1000
				Compliance	1000
				Identity Management	800
				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 off-boarding 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



1800 Chapel Avenue West
Suite 360
Cheery Hill, NJ 08002

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

William J. Elkins
Chief Technology Officer