

Cybersecurity

Self-Assessment Tool

*Using the National Institute of Standards and Technology Cybersecurity Framework*

**Disclaimer:** The information contained in this tool is provided for informational purposes and does not constitute legal advice. This tool is not intended to be used for making business, legal, or financial decisions.

***Commissioners***



***Craig P. Tanio, MD, MBA, Chair***

|  |  |
| --- | --- |
| Frances B. Phillips, RN, MHA, Vice Chair Health Care Consultant  John E. Fleig, Jr.  Chief Operating Officer  UnitedHealthcare MidAtlantic Health Plan  Elizabeth A. Hafey, Esq. Associate Miles & Stockbridge P.C.  Jeffrey Metz, MBA, LNHA  President and Administrator  Egle Nursing and Rehab Center  Robert Emmet Moffit, PhD  Senior Fellow  Health Policy Studies  Heritage Foundation  Gerard S. O’Connor, MD  General Surgeon in Private Practice  Michael J. O’Grady, PhD Principal, Health Policy LLC, and  Senior Fellow, National Opinion Research Center (NORC) at the University of Chicago | Andrew N. Pollak, MD  Professor and Chair Department of Orthopaedics University of Maryland School of Medicine Chief of Orthopaedics University of Maryland Medical System  Randolph S. Sergent, Esq. Vice President and Deputy General Counsel CareFirst BlueCross BlueShield  Diane Stollenwerk, MPP  President  StollenWerks, Inc.  Stephen B. Thomas, PhD  Professor of Health Services Administration  School of Public Health  Director, Maryland Center for Health Equity  University of Maryland, College Park  Cassandra Tomarchio Business Operations Manager Enterprise Information Systems Directorate US Army Communications Electronics Command  Adam J. Weinstein, MD Medical Director Nephrology and Transplant Services Shore Health System  Maureen Carr-York, Esq.  Public Health Nurse and Health Care Attorney  Anne Arundel County |

***CEO and Founder, Rezilir Healh***

**Table of Contents**

Overview3

About the NIST CSF3

How to Use this Tool4

Description of Readiness Levels4

Scoring Overview4

Resources5

Assessment Questions Sections6-22

Identify6

Protect10

Detect15

Respond18

Recover21

Scoring23

About MHCC25

Acknowledgements25

Glossary of Terms26

This tool was compiled by Justine Springer, Program Manager, within the Center for Health Information Technology & Innovative Care Delivery under the direction of the Center Director, David Sharp, Ph.D. For information on this tool, please contact Justine Springer at 410-764-3777 or by email at justine.springer@maryland.gov.

**Overview**

An increase in cyber threats is causing most health care providers to take a broader approach to assessing cybersecurity readiness, including response and recovery protocols to help mitigate the impact of a cyber-attack. Assessing cybersecurity readiness is essential to ensuring that an organization’s critical infrastructure is adequately protected. The impact of a cyber-attack can include: disruptions in accessing electronic health record systems; compromised functioning of networked medical devices; financial consequences associated with recovery; damage to an organization’s reputation; and creation of consumer fear about the security of their personal health information. This Cybersecurity Self-Assessment Tool (tool) was developed by the Maryland Health Care Commission (MHCC) to assist small health care providers (providers) in identifying gaps and potential risks in their cybersecurity processes. The tool can also be used to provide guidance in the development and implementation of cyber protections where cybersecurity processes do not currently exist. The tool was developed using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[[1]](#footnote-1), which assembles standards, guidelines, and practices to evaluate cybersecurity. The tool guides users through assessing the organizational processes that address the five core functions of the NIST CSF: 1) identify, 2) protect, 3) detect, 4) respond, and 5) recover. Results can be used by an organization to assess their risk of a cyber-attack and to develop processes that mitigate risk.

**About the NIST CSF**

In response to growing cyber threats, an Executive Order entitled *Improving Critical Infrastructure Cybersecurity* (order), issued in 2013, called for a set of industry standards and best practices for managing cyber risks. The order resulted in the development of the NIST CSF. The NIST CSF enables providers to assess their cybersecurity environment, regardless of size, degree of risk, or experience. It also offers voluntary guidance to providers to understand, select, and implement cybersecurity controls. Each of the five NIST CSF functions are divided into categories that address each of the requirements. Providers using this tool are encouraged to review the NIST CSF at: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework/).

**How to Use this Tool**

Users of the tool assess their organization’s cybersecurity readiness by selecting from one of four options that most accurately reflects the organization’s readiness for meeting best practices: informal, developing, established, or N/A. The example below provides users with a description of the different components of the assessment questions.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Management (ID.AM):** *Assess organizational assets, such as data, personnel, devices, systems, and facilities, to determine if they are managed in a manner consistent with their level of importance to the cybersecurity of the organization.* | | | | | |
| **ID.AM** | **Processes to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| 1 | Inventory physical devices and systems (e.g., computers, mobile devices, networked medical devices, virtual machines, etc.)? |  |  |  |  |

References NIST subcategory

NIST category being assessed

Question to assess readiness for each component of the NIST subcategory

Select **one** answer that most accurately reflects organization readiness in establishing and implementing cybersecurity processes

**Description of Readiness Levels**

**Informal:** No formal processes exist. Standardization of organizational processes has not yet occurred.

**Developing:** Formal processes are in development. The organization is evaluating risks and identifying appropriate protocols that are informed by the risk evaluation.

**Established:** Formal processes that are standardized across the organization have been established. The organization continuously evaluates risks and adapts processes in response to changes in its cybersecurity environment.

**N/A**: Not applicable to the organization.

**Scoring** **Overview**

After the completion of each function, users tabulate their results by counting the number of responses for each readiness level in each function. Users then calculate a percent for that function by using the number answered “Established” and dividing by the total number of questions answered. The percent is circled on the “Readiness Indicator” scale for each function to provide the user with an overall assessment of the performance in that function. After completing all five functions, users can total their scores and calculate an “Overall Readiness Indicator.” More information on scoring can be found in the scoring section on page 23 of this document.

**Resources**

**Glossary**

A glossary of terms is included as an attachment to assist users in completing the tool. The glossary defines key terms found in this document.

**Other Resources**

1. *Baldrige Cybersecurity Excellence Builder-DRAFT*, National Institute of Standards and Technology. Available at: [www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf](http://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf)
2. *Security Risk Assessment Tool,* HealthIT.gov. Available at: [www.healthit.gov/providers-professionals/security-risk-assessment-tool](http://www.healthit.gov/providers-professionals/security-risk-assessment-tool)
3. *Framework for Improving Critical Infrastructure Cybersecurity Version 1*, National Institute of Standards and Technology. Available at: [www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf](http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)
4. *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology Special Publication 800-53 Revision 4. Available at: [nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf](file:///\\ADMIN2\dev\EDI\CIO%20Listing\Cybersecurity\Resources\Assessment%20Tool\nvlpubs.nist.gov\nistpubs\SpecialPublications\NIST.SP.800-53r4.pdf)
5. *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework,* Health and Human Services. Available at: [www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf](http://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf)

Section 1:

**Identify**

**Identify (ID)**

The NIST CSF “Identify” function helps a provider assess their systems, assets, data, business context, and resources to understand and manage cybersecurity risk. The components of the Identify function are the foundation for cybersecurity readiness. Identifying the components that are critical to the organization’s infrastructure helps to focus and prioritize development of cybersecurity processes that are consistent with its risk management strategy and organizational needs.

**Assessment Questions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Management (ID.AM):** *Assess organizational assets, such as data, personnel, devices, systems, and facilities, to determine if they are managed in a manner consistent with their level of importance to the cybersecurity of the organization*. | | | | | |
| **ID.AM** | **Implementing a processes to:** | **Readiness** | | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Inventory physical devices and systems (e.g., computers, mobile devices, networked medical devices, virtual machines, etc.) |  |  |  |  |
| *2* | Inventory software platforms and applications (e.g., Microsoft Windows, OS X (Mac OX), Linux, Amiga OX, etc.) |  |  |  |  |
| *3* | Document the organization’s communication and data flows |  |  |  |  |
| *4* | Catalogue externally owned or operated communication systems (e.g., computing devices, wireless networks, and cloud services) |  |  |  |  |
| *5* | Prioritize resources (e.g., hardware devices, data, and software) based on their impact to cybersecurity |  |  |  |  |
| *6* | Outline cybersecurity roles and responsibilities for all employees and third-parties (e.g., suppliers, customers, and contractors) |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Environment (ID.BE):** *Identify and prioritize the organization’s mission, objectives, stakeholders, and activities to inform the cybersecurity roles, responsibilities, and risk management decisions.* | | | | | |
| **ID.BE** | **Identified and communicated:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Its function in the supply chain |  |  |  |  |
| *2* | Its position in critical infrastructure and the industry |  |  |  |  |
| *3* | Information on its mission, objectives, and activities |  |  |  |  |
| *4* | Dependencies and critical functions for the delivery of critical services |  |  |  |  |
| *5* | Recovery requirements and protocols to support critical services |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Governance (ID.GV):** *Assess the organization’s policies and procedures to manage and monitor the operational, environmental, and regulatory requirements to inform and manage the organization’s cybersecurity risk.* | | | | | |
| **ID.GV** | **Implemented processes for:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Information security |  |  |  |  |
| *2* | Coordination and alignment of internal and external roles and responsibilities |  |  |  |  |
| *3* | Legal and regulatory requirements |  |  |  |  |
| *4* | Governance and risk management processes |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Assessment (ID.RA):** *Assess the organization’s cybersecurity risk as it pertains to the organizational operations, assets, and individuals.* | | | | | |
| **ID.RA** | **Implementing a processes to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Identify and document asset vulnerabilities |  |  |  |  |
| *2* | Receive and share threat and vulnerability information with external organizations |  |  |  |  |
| *3* | Document internal and external threats |  |  |  |  |
| *4* | Identify potential business impacts (e.g., likelihood and potential harm to the organization resulting from unauthorized access) |  |  |  |  |
| *5* | Evaluate risks of threats, vulnerabilities, and potential business impact |  |  |  |  |
| *6* | Prioritize and respond to identified cybersecurity risks |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Management Strategy (ID.RM):** *Assess the organization’s established priorities, constraints, risk tolerances, and assumptions, which are used to support the organization’s risk decisions.* | | | | | |
| **ID.RM** | **Identified and communicated:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Risk management processes approved by organizational stakeholders |  |  |  |  |
| *2* | Organizational risk tolerance |  |  |  |  |
| *3* | Risk informed processes to determine the acceptable level of risk for the organization’s cybersecurity threats |  |  |  |  |

Please see “Scoring” on page 23 to calculate your score for “Identify.”

Section 2:

**Protect**

**Protect (PR)**

The NIST CSF “Protect” function aims to ensure continuity of critical infrastructure services. This function provides the framework for providers to develop and implement the appropriate safeguards to limit or contain the potential impact of a cybersecurity event. The organizational safeguards assessed include access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

**Assessment Questions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Access Control (PR.AC):** *Assesses the organizational processes to limit access to assets and facilities to authorized users, devices, activities, and transactions.* | | | | | |
| **PR.AC** | **Appropriate safeguards to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Manage identities and credentials for authorized devices and users |  |  |  |  |
| *2* | Manage and protect physical access to assets |  |  |  |  |
| *3* | Manage remote access |  |  |  |  |
| *4* | Manage access permissions (includes least privilege and separation of duties) |  |  |  |  |
| *5* | Protect network integrity and utilize appropriate network segregation |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Awareness and Training (PR.AT):** *Assesses the adequacy of the cybersecurity awareness education and training necessary for personnel and partners to perform their information security related duties and responsibilities.* | | | | | |
| **PR.AT** | **Process to evaluate and document:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | All users are informed and trained |  |  |  |  |
| *2* | All privileged users understand their roles and responsibilities |  |  |  |  |
| *3* | All third party stakeholders understand their roles and responsibilities |  |  |  |  |
| *4* | Senior executives understand their roles and responsibilities |  |  |  |  |
| *5* | Physical and information security personnel understand their roles and responsibilities |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data Security (PR.DS):** *Appropriately manage all information and records at the organization in accordance with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.* | | | | | |
| **PR.DS** | **Appropriate safeguards to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Protect data-at-rest |  |  |  |  |
| *2* | Protect data-in-transit |  |  |  |  |
| *3* | Formally manage assets during removal, transfer, and disposition |  |  |  |  |
| *4* | Ensure adequate capacity to maintain data availability |  |  |  |  |
| *5* | Protect against data leaks |  |  |  |  |
| *6* | Verify software, firmware, and information integrity |  |  |  |  |
| *7* | Maintain separation between the development and testing environment(s), and the production environment |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Information Protection Processes and Procedures (PR.IP):** *The organization’s security policies, processes, and procedures are maintained and adequately manage protection of information systems and assets.* | | | | | |
| **PR.IP** | **Implemented a process to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Create and maintain baseline configuration of information technology and systems that control production and distribution |  |  |  |  |
| *2* | Manage systems through a System Development Life Cycle |  |  |  |  |
| *3* | Control system configuration changes |  |  |  |  |
| *4* | Maintain and test information backup procedures |  |  |  |  |
| *5* | Adhere to policies and regulations for the physical operating environment for organizational assets |  |  |  |  |
| *6* | Destroy data in accordance with policy |  |  |  |  |
| *7* | Continuously improve protection processes |  |  |  |  |
| *8* | Appropriately share the effectiveness of technology used for protection of systems and assets |  |  |  |  |
| *9* | Manage response and recovery plans |  |  |  |  |
| *10* | Test response and recovery plans |  |  |  |  |
| *11* | Include cybersecurity in human resources practices |  |  |  |  |
| *12* | Develop and implement a vulnerability management plan |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Maintenance (PR.MA):** *Maintenance and repairs are performed for all industrial controls and information system components.* | | | | | |
| **PR.MA** | **Implemented a process to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Use approved and controlled tools to timely perform, repair, and log maintenance and repairs |  |  |  |  |
| *2* | Approve, log, and perform all remote maintenance of organizational assets to prevent unauthorized access |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Protective Technology (PR.PT):** *The security and resilience of systems and assets are managed through the use of technology security solutions that are consistent with related policies, procedures, and agreements.* | | | | | |
| **PR.PT** | **Implemented a process to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Create, document, implement, and review audit/log records |  |  |  |  |
| *2* | Protect and restrict use of removable media |  |  |  |  |
| *3* | Limit access systems and assets to the minimal level necessary to maintain normal functioning |  |  |  |  |
| *4* | Protect communications and control networks |  |  |  |  |

Please see “Scoring” on page 23 to calculate your score for “Protect.”

Section 3:

**Detect**

**Detect (DE)**

The NIST CSF “Detect” function aims to ensure cybersecurity incidents can be identified in a timely manner. This function assists providers in assessing procedures to rapidly identify cyber events, test detection processes, analyze data to understand attack targets and methods, and inform improvements to organizational processes. The organizational safeguards assessed include anomalies and events, security continuous monitoring, and detection processes.

**Assessment Questions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Anomalies and Events (DE.AE):** *Assesses the organization’s ability to detect unusual activity in a timely manner and understand potential impacts of cyber events.* | | | | | |
| **DE.AE** | **Appropriate safeguards to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Establish and manage baseline network operations and data flows for users and systems |  |  |  |  |
| *2* | Analyze detected events to understand attack targets and methods |  |  |  |  |
| *3* | Combine data from events and link to multiple sources |  |  |  |  |
| *4* | Determine impact of events |  |  |  |  |
| *5* | Establish incident alert levels |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Security Continuous Monitoring (DE.CM):** *Assesses organizational processes for routinely monitoring information systems and assets to identify cybersecurity events and continuously test the effectiveness of current preventative measures.* | | | | | |
| **DE.CM** | **Processes to monitor:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | The network to detect cybersecurity events |  |  |  |  |
| *2* | The physical environment to detect cybersecurity events |  |  |  |  |
| *3* | Personnel activity to detect cybersecurity events |  |  |  |  |
| *4* | For malicious code |  |  |  |  |
| *5* | For unauthorized mobile code |  |  |  |  |
| *6* | External service provider activity to detect cybersecurity events |  |  |  |  |
| *7* | Access by unauthorized personnel, connections, devices, and software |  |  |  |  |
| *8* | System vulnerability by performing vulnerability scans |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Detection Processes (DE.DP):** *Assess the maintenance and testing of an organization’s detection processes and procedures to ensure timely and adequate awareness of unusual events.* | | | | | |
| **DE.DP** | **Safeguards to ensure:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Accountability for detection by having well-defined personnel roles and responsibilities |  |  |  |  |
| *2* | Compliance with applicable organizational requirements for detection activities |  |  |  |  |
| *3* | Testing of detection processes |  |  |  |  |
| *4* | Communication of information pertaining to cyber events to appropriate parties |  |  |  |  |
| *5* | Continuous improvement of detection processes |  |  |  |  |

Please see “Scoring” on page 23 to calculate your score for “Detect.”

Section 4:

**Respond**

**Respond (RS)**

The NIST CSF “Respond” function aims to assist providers to contain the impact of a potential cybersecurity event. This function supports providers in assessing current processes in place to respond to a detected cybersecurity event. The organizational safeguards assessed include: response planning, communications, analysis, mitigation, and improvements.

**Assessment Questions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Response Planning (RS.RP):***Assesses the organization’s ability to execute and maintain response processes and procedures for responding timely to detected cybersecurity events.* | | | | | |
| **RS.RP** | **Appropriate processes to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Execute a response plan during or after a detected cyber event |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Communications (RS.CO):** *Assesses the organization’s coordination of response activities with the appropriate internal and external stakeholders, including support from law enforcement agencies, as applicable.* | | | | | |
| **RS.CO** | **Process to support:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Personnel training regarding roles and order of operations |  |  |  |  |
| *2* | Reporting of events according to established criteria |  |  |  |  |
| *3* | Sharing information in accordance with response plans |  |  |  |  |
| *4* | Stakeholder coordination to ensure execution of response plans |  |  |  |  |
| *5* | Voluntary information sharing with external stakeholders for broad cybersecurity awareness |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Analysis (RS.AN):** *Conducts analyses of response processes to ensure appropriate response, and to support recovery activities.* | | | | | |
| **RS.AN** | **Appropriate processes to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Investigate notifications from detection systems |  |  |  |  |
| *2* | Understand the impact of an incident |  |  |  |  |
| *3* | Perform forensics |  |  |  |  |
| *4* | Categorize incidents in accordance with response plans |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mitigation (RS.MI):** *Has processes to contain, mitigate the effects of, and eradicate a cybersecurity event.* | | | | | |
| **RS.MI** | **Appropriate safeguards to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Contain events |  |  |  |  |
| *2* | Mitigate events |  |  |  |  |
| *3* | Mitigate or document the acceptance of risks for newly identified vulnerabilities |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Improvements (RS.IM):** *Utilizes lessons learned from detection and response activities to improve processes.* | | | | | |
| **RS.IM** | **Response plans:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Incorporate lessons learned |  |  |  |  |
| *2* | Are updated regularly to meet the needs of a changing cyber landscape |  |  |  |  |

Please see “Scoring” on page 23 to calculate your score for “Respond.”

Section 5:

**Recover**

**Recover (RC)**

The NIST CSF “Recover” function aims to support a provider in rapidly recovering and mitigating the long term impact of a cybersecurity event. This function supports providers in assessing the processes to maintain resiliency plans and support restoration of services impacted during an event. The organizational safeguards assessed include recovery planning, improvements, and communications.

**Assessment Questions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Recovery Planning (RC.RP):***Assesses the organizational ability to execute and maintain recovery processes and procedures to ensure timely response to detected cybersecurity events.* | | | | | |
| **RC.RP** | **Appropriate processes to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Execute a recovery plan during or after an event |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Improvements (RC.IM):** *Assesses the organization’s processes to improve recovery plans by incorporating lessons learned.* | | | | | |
| **RC.IM** | **Recovery Plans:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Incorporate lessons learned |  |  |  |  |
| *2* | Are updated regularly to meet the needs of a changing cyber landscape |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Communications (RC.CO):**  *Assesses the organizations processes to coordinate restoration activities with internal and external parties, including coordinating centers, Internet Service Providers, cyber-attack victims, and vendors.* | | | | | |
| **RC.CO** | **Appropriate processes to:** | **Readiness** | | | |
| **Informal** | **Developing** | **Established** | **N/A** |
| *1* | Manage public relations |  |  |  |  |
| *2* | Repair reputation |  |  |  |  |
| *3* | Internally communicate recovery activities |  |  |  |  |

Please see “Scoring” on page 23 to calculate your score for “Protect.”

**Scor****ing**

About the score

The score is meant to serve as an indicator of an organization’s cybersecurity readiness. By using the readiness indicator, providers can identify gaps in their existing cybersecurity processes and use the information to enhance existing cybersecurity initiatives. For organizations where cybersecurity initiatives have not been formally established, the readiness indicator can help identify areas where best practices for cybersecurity preparedness need to be developed.

Calculate the score

1. Count the number of answers selected for each readiness level for each function and enter the number in the corresponding cell.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Readiness Level** | **Identify** | **Protect** | **Detect** | **Respond** | **Recover** | **Readiness Level Total** |
| Informal |  |  |  |  |  |  |
| Developing |  |  |  |  |  |  |
| Established |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Function Total |  |  |  |  |  |  |

1. Using the numbers from the “Number Answered” column in the above chart, calculate your *Readiness Percent* score by dividing the number of questions answered “Established” by the total number of questions answered.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Identify** | **Protect** | **Detect** | **Respond** | **Recover** | **Total** |
| **Answered “Established** |  |  |  |  |  |  |
| **Total Number Answered** |  |  |  |  |  |  |
| **Readiness percent** |  |  |  |  |  |  |

1. Circle the “Readiness Percent” on the scale below

|  |
| --- |
| **Readiness Indicator** |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Identify** | **0%** | **10%** | **20%** | **30%** | | **40%** | **50%** | **60%** | **70%** | | **80%** | **90%** | **100%** | |  |  |  |  |  | |  |  |  |  | |  |  |  | | **Protect** | **0%** | **10%** | **20%** | **30%** | | **40%** | **50%** | **60%** | **70%** | | **80%** | **90%** | **100%** | |  |  |  |  |  | |  |  |  |  | |  |  |  | | **Detect** | **0%** | **10%** | **20%** | **30%** | | **40%** | **50%** | **60%** | **70%** | | **80%** | **90%** | **100%** | |  |  |  |  |  | |  |  |  |  | |  |  |  | | **Respond** | **0%** | **10%** | **20%** | **30%** | | **40%** | **50%** | **60%** | **70%** | | **80%** | **90%** | **100%** | |  |  |  |  |  | |  |  |  |  | |  |  |  | | **Recover** | **0%** | **10%** | **20%** | **30%** | | **40%** | **50%** | **60%** | **70%** | | **80%** | **90%** | **100%** | |  |  |  |  |  | |  |  |  |  | |  |  |  | | **Overall** | **0%** | **10%** | **20%** | **30%** | | **40%** | **50%** | **60%** | **70%** | | **80%** | **90%** | **100%** | |  | **Partial** | | | | **Moderate** | | | | | **Advanced** | | | | |

**Description of Readiness Indicator Levels**

**Partial:** Minimal development of formal processes and diffusion of cybersecurity practices throughout the organization.

**Moderate:** Some formalized processes are established and diffused throughout the organization. Processes are being developed to address identified gaps.

**Advanced:** Formalized organization-wide processes to address the majority of cybersecurity risks are in place and diffused throughout the organization.

**About MHCC**

The Maryland Health Care Commission (MHCC) is an independent regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policy makers, purchasers, providers and the public. The MHCC is responsible for advancing health information technology statewide and fostering innovation in a way that balances the need for information sharing with the need for strong privacy and security policies.

**Acknowledgements**

The MHCC appreciates the contribution made by hospital Chief Information Officers and Chief Information Security Officers in developing the tool. The effort from hospitals in developing a tool that can be valuable to small health care providers is commendable.

**Glossary of Terms**

1. **Asset:** Property owned by an organization that is regarded as having value.
2. **Authorized:** An individual or system’s approval to access and operate at the organization and to explicitly accept the associated risk to organizational operations, assets, individuals, and other organizations based on the security controls.
3. **Catalogue:** A complete list of communication systems used by the organization that **are not** owned or controlled by the organization.
4. **Communications:** The transmission of data from one computer or device to another.
5. **Communication systems:** A mechanism for transferring data between persons and equipment.
6. **Configuration:** The arrangement or set-up of a computer’s hardware and software.
7. **Control networks:** Collection of devices or data points that monitor, sense, and control the cyber environment.
8. **Critical infrastructure:** System or assets, both physical and virtual, so vital to the organization that the incapacity or destruction would jeopardize the security and continued operation of the organization.
9. **Critical functions:** Processes and activities that are so vital to the infrastructure of the organization that, if interrupted or destroyed, would jeopardize the security and continued operation of the organization.
10. **Critical services**: Services that are so vital to the infrastructure of the organization that, if interrupted or destroyed, would jeopardize security and continued operation of the organization.
11. **Cybersecurit**y: The technologies, processes, and practices that are designed to protect the cyber environment of an organization’s critical infrastructure.
12. **Data flows:** Method for how data moves from one system to another through an organization.
13. **External service provider:** A separate legal entity that provides services, such as software development, to another company through a contract.
14. **External threat:** A threat that originates from outside the organization (e.g., a hacker, a virus, etc.).
15. **Firmware:** Permanent software programmed into read-only memory.
16. **Forensics**: Tests or techniques that are performed to detect a cybersecurity event.
17. **Human resources practice:** Policies surrounding personnel screening, termination, transfer, access agreements, third party access, and sanctions.
18. **Incident alert levels:** A set of predefined conditions that when met trigger an alert.
19. **Information security:** Processes that are designed and implemented to protect any type of confidential, private, and sensitive information or data from unauthorized access, use, disclosure, destruction, or modification.
20. **Information security personnel:** Personnel who are responsible for the security of the informational assets at the organization.
21. **Information system components:** A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents an essential piece used to build an information system.
22. **Internal threat:** A threat that originates from within the organization (e.g., employee, system vulnerability, etc.).
23. **Inventory:** A complete list of all physical devices, systems, and software that are **owned** and operated by the organization.
24. **Least privilege:** Principle that allows access only for authorized users or processes acting on behalf of users, which are necessary to accomplish assigned tasks consistent with organizational processes.
25. **Malicious code:** Part of a software system or script that is intended to breach security or damage a system that cannot be adequately controlled by traditional antivirus software.
26. **Mobile code:**  Program, application, or content that can be moved electronically through the use of a network or storage device to locally execute code from another computer system.
27. **Networked Medical Devices:** Instrument or machine intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease that is connected to the organization’s computer network.
28. **Network operations:** Process to manage and control computer networks**.**
29. **Network segregation:** Dividing a network in smaller subnetworks or network segments to enhance security by increasing the difficulty for an attacker to discover the network structure, limiting the spread of intrusions to other network segments, and increasing access control by limiting visitor access or access to sensitive assets.
30. **Organizational operations:** Activities involved in the day to day function of the organization.
31. **Physical environment:** Tangible components of the organization outside of the cyber environment, such as facilities, equipment, supplies, etc.
32. **Physical operating environment:** The environment in which users run application software consisting of a user interface and an application programming interface.
33. **Privileged users:** Authorized users or processes acting on behalf of users who are given access to an organizational system or process.
34. **Production environment:** The forum where software and other products are put into operation for their intended use by the end users.
35. **Recovery plans:** A component of the organizational program for achieving continuity of organizational operations following a disaster (e.g., Incident Recovery and Disaster Recovery).
36. **Response plans:** A component of the organizational program that outlines an organized approach for addressing and managing a cyber attack to limit damage and reduce recovery time and costs.
37. **Removable media:** Any type of storage device that can be removed while maintaining operation of the system, such as diskettes, external/removable hard disk drives, flash/USB drives, compact disks, and digital video disks).
38. **Risk management:** The process of identifying and analyzing cybersecurity threats, policies and procedures to mitigate uncertainty in cybersecurity decisions.
39. **Security policies:** Documented procedures that state how an organization plans to address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities to protect the organization’s assets.
40. **Separation of duties:** The practice of dividing and conducting mission, information system, and security functions among different individuals and roles to reduce potential abuse of authorized privileges and malicious activity.
41. **Small health care provider:** An individual who practices at an organization or practice not owned by a large hospital or health system.
42. **Supply chain:** Linked set of resources and processes between organizations, people, activities, information, and resources that extends through design, development, manufacturing, processing, handling, and delivery of products and services from the supplier to the acquirer.
43. **Systems:** The organization’s hardware and software components required to operate the organization’s devices, such as computers, mobile devices, networked medical devices, virtual machines, etc.
44. **System Development Life Cycle:** Process for planning, creating, testing, and deploying an information system that provides the foundation for the successful development, implementation, and operation of organizational information systems.
45. **Third party stakeholders:** Include suppliers, customers, and partners that provide information system development, information technology services, outsourced applications, and network and security management.
46. **Unauthorized:** An individual or system who is not approved to access or operate a system, device, or network which incurs an associated risk to organizational operations, assets, individuals, and other organizations.
47. **Users:** Individuals who utilize a computer or network service, generally without the technical expertise required for complete understanding of its operation.
48. **Vulnerability scans:** Inspects devices, systems, and networks to detect and classify system weaknesses and predict effectiveness of remedies.

**David Sharp, Ph.D.**

**Director**

**Center for Health Information Technology**

**and Innovative Care Delivery**



4160 Patterson Avenue

Baltimore, MD 21215

410-764-3460

www.mhcc.maryland.gov

1. The Cybersecurity Self-Assessment Tool uses the functions, categories, and subcategories developed by NIST. Descriptions in this document contain language used in the “Framework for Improving Critical Infrastructure Cybersecurity Version 1.0” developed by NIST. A copy of the document can be accessed at: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> [↑](#footnote-ref-1)