Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

Clearwater

Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing

July 2023

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Cyber Briefings are eligible for HIMSS & CHIME CE credit
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Clearwater

Agenda

- Cyber update
- NIST CSF 2.0

Clearwater

July's Speakers

Steve Cagle, MBA, HCISSP
Chief Executive Officer

Dave Bailey, CISSP
VP, Consulting Services

Rick Lemay
Director, Consulting Services for Hospitals & Health Systems

Clearwater

Cyber Update

Steve Cagle

Halfway Through 2023 – Where We Stand

41m Individuals' records compromised 6/30/23[1]

56% Increase in ransomware attacks May 2023 vs 2022[2]

19 Hospitals systems hit with ransomware in 2023[3]

30% Revenue lost due to a ransomware attack for a small healthcare provider[4]

1 Midyear Health Data Breach Analysis: The Top Culprits (databreachtoday.com)
2 https://www.nccgroup.com/media/sznpjuy5/may-threat-pulse-2023.pdf
3 https://www.infosecurity-magazine.com/news/thirtythree-us-hospitals/
4 https://www.hipaajournal.com/healthcare-ransomware-attacks-threaten-up-to-30-of-operating-income/

Clearwater

Recent Large Healthcare Breaches

Managed Care of North America Hacking Incident Impacts 8.9 Million Individuals

Posted By Steve Alder on May 30, 2023

Victim of LockBit ransomware group. Reported May 30.

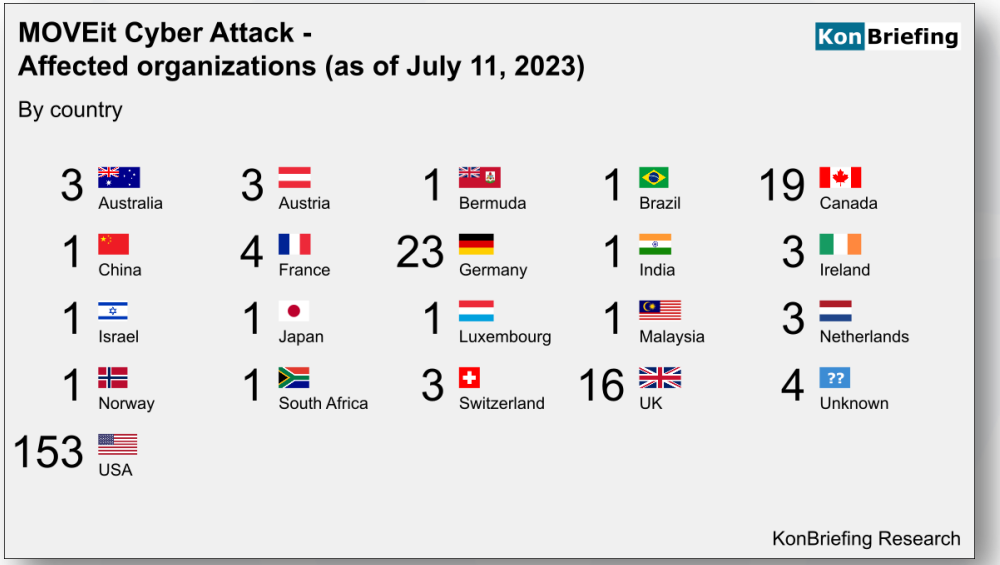
HCA Healthcare Suffers Data Breach, 11M Patients Impacted

An unauthorized party stole a list of information used for email messages to patients and posted it on an online forum, HCA Healthcare stated in its data breach notice.

Largest health data breach of 2023. Reported July 10.

MOVEit Vulnerability – CL0P Ransomware Gang Campaign

- Starting end of May Cl0p ransomware gang, mass-exploited a zero-day vulnerability in the MOVEit Transfer product, tracked as CVE-2023-34362, to steal data from large organizations worldwide.
- In total, 3 additional vulnerabilities reported – patches available
- Hundreds of victims including federal government, state government, and healthcare covered entities and business associates



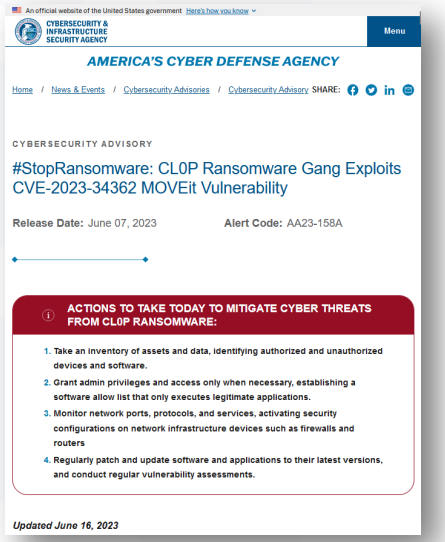
Data and graphic from KonBriefing Research as of July 10, 2023.
https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html

Clearwater

Recent Notable Advisories

- June 14
- Details observed activity in LockBit ransomware incidents
- Advisory provides recommendations for identifying and stopping Lockbit

Link to Advisory



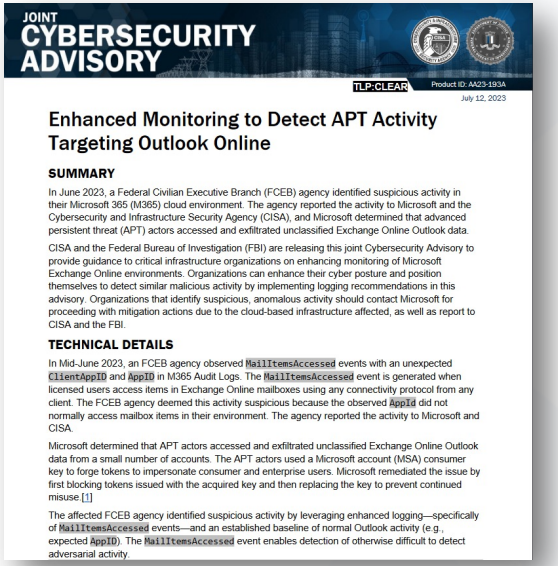
- June7
- Recommended actions and mitigations to protect against CL0P exploiting MOVEit
- Disseminates known CL0P ransomware IOCs and TTPs identified through FBI investigations

Link to Advisory

Clearwater

Notable Advisories (cont).

A Chinese hacking group (Storm-0558) has breached Microsoft email accounts of more than two dozen organizations worldwide, including U.S. and Western European government agencies, according to Microsoft.



JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA23-193A

July 12, 2023

Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

SUMMARY

In June 2023, a Federal Civilian Executive Branch (FCEB) agency identified suspicious activity in their Microsoft 365 (M365) cloud environment. The agency reported the activity to Microsoft and the Cybersecurity and Infrastructure Security Agency (CISA), and Microsoft determined that advanced persistent threat (APT) actors accessed and exfiltrated unclassified Exchange Online Outlook data.

CISA and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory to provide guidance to critical infrastructure organizations on enhancing monitoring of Microsoft Exchange Online environments. Organizations can enhance their cyber posture and position themselves to detect similar malicious activity by implementing logging recommendations in this advisory. Organizations that identify suspicious, anomalous activity should contact Microsoft for proceeding with mitigation actions due to the cloud-based infrastructure affected, as well as report to CISA and the FBI.

TECHNICAL DETAILS

In Mid-June 2023, an FCEB agency observed `MailItemsAccessed` events with an unexpected `ClientAppID` and `AppID` in M365 Audit Logs. The `MailItemsAccessed` event is generated when licensed users access items in Exchange Online mailboxes using any connectivity protocol from any client. The FCEB agency deemed this activity suspicious because the observed `AppId` did not normally access mailbox items in their environment. The agency reported the activity to Microsoft and CISA.

Microsoft determined that APT actors accessed and exfiltrated unclassified Exchange Online Outlook data from a small number of accounts. The APT actors used a Microsoft account (MSA) consumer key to forge tokens to impersonate consumer and enterprise users. Microsoft remediated the issue by first blocking tokens issued with the acquired key and then replacing the key to prevent continued misuse.[1]

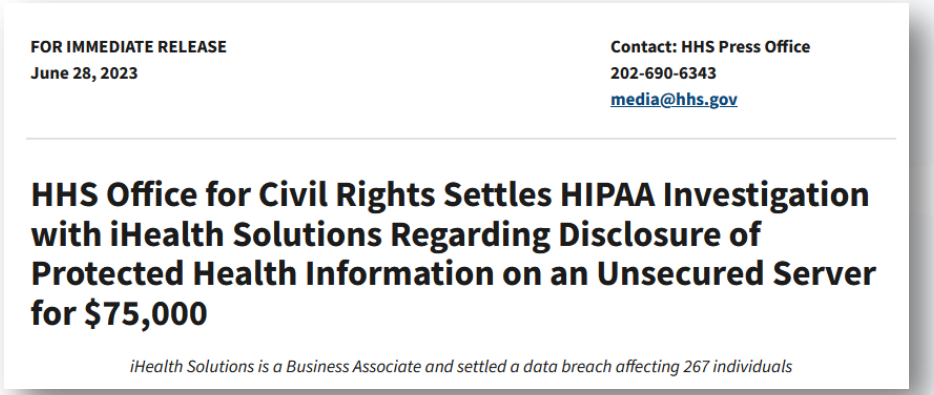
The affected FCEB agency identified suspicious activity by leveraging enhanced logging—specifically of `MailItemsAccessed` events—and an established baseline of normal Outlook activity (e.g., expected `AppID`). The `MailItemsAccessed` event enables detection of otherwise difficult to detect adversarial activity.

- July 12
- Guidance to critical infrastructure organizations on enhancing monitoring of Microsoft Exchange Online environments (logging)
- Provides additional cloud mitigation recommendations

Link to Advisory

Clearwater

OCR Enforcement Since Last Cyber Briefing



FOR IMMEDIATE RELEASE
June 28, 2023

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Office for Civil Rights Settles HIPAA Investigation with iHealth Solutions Regarding Disclosure of Protected Health Information on an Unsecured Server for $75,000

iHealth Solutions is a Business Associate and settled a data breach affecting 267 individuals

"OCR's investigation found evidence of the potential failure by iHealth Solutions to have in place **an analysis to determine risks and vulnerabilities** to electronic protected health information across the organization"

Clearwater

Additional Recommendations For Mature Organizations to Address Current Threat Environment

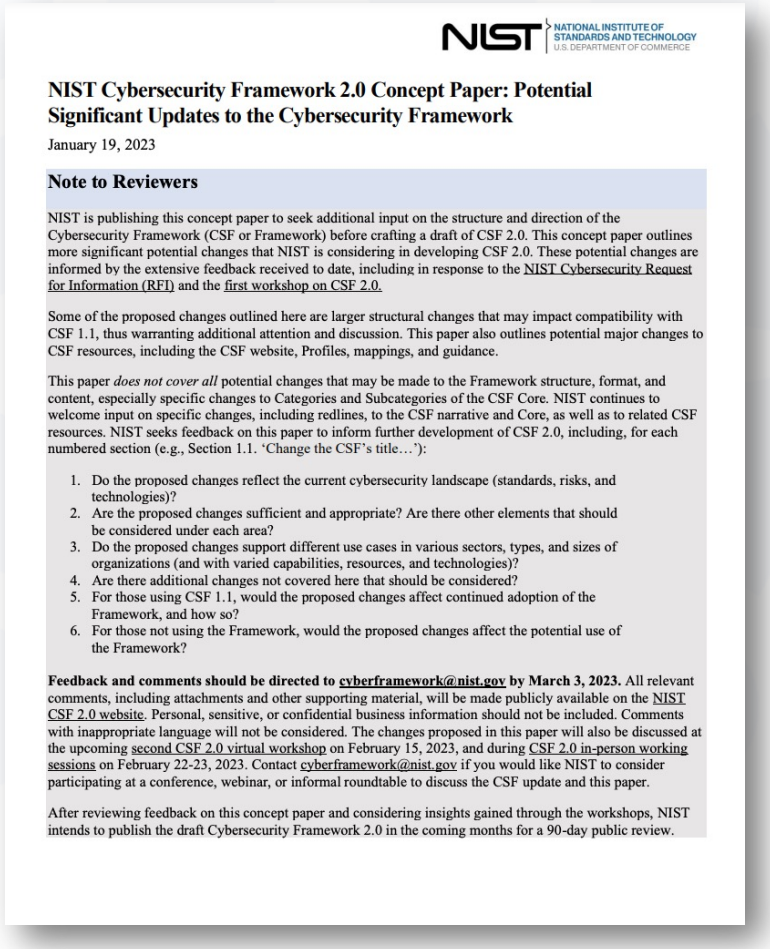
- Know where your data is! Ensure Risk Analysis is up to date and has analyzed specific risks and controls at the information systems level
- Respond to high risks through diligent risk treatment and risk management processes
- Conduct on-going vulnerability management – not just periodic scans – and patch critical or high vulnerabilities
- Monitor and act on-going threat intelligence and alerts from H-ISAC, CISA, and other agencies
- Ensure that the security controls you have in place are working as you expect
- Assess high impact third parties for risk, including asking questions about their vulnerability management programs and risk analysis
- Develop and test incident response plans

NIST CSF 2.0

Impacts to Healthcare Security Programs

Update to the NIST Cybersecurity Framework

- NIST v2.0 in draft and public comment period
- Planned release in early 2024
- Emphasis on Governance & Supply Chain Risk Management
- Notable new categories: Organizational Context, Platform Security, and Technology Infrastructure Resilience



NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

January 19, 2023

Note to Reviewers

NIST is publishing this concept paper to seek additional input on the structure and direction of the Cybersecurity Framework (CSF or Framework) before crafting a draft of CSF 2.0. This concept paper outlines more significant potential changes that NIST is considering in developing CSF 2.0. These potential changes are informed by the extensive feedback received to date, including in response to the NIST Cybersecurity Request for Information (RFI) and the first workshop on CSF 2.0.

Some of the proposed changes outlined here are larger structural changes that may impact compatibility with CSF 1.1, thus warranting additional attention and discussion. This paper also outlines potential major changes to CSF resources, including the CSF website, Profiles, mappings, and guidance.

This paper *does not cover all* potential changes that may be made to the Framework structure, format, and content, especially specific changes to Categories and Subcategories of the CSF Core. NIST continues to welcome input on specific changes, including redlines, to the CSF narrative and Core, as well as to related CSF resources. NIST seeks feedback on this paper to inform further development of CSF 2.0, including, for each numbered section (e.g., Section 1.1. 'Change the CSF's title…'):

1. Do the proposed changes reflect the current cybersecurity landscape (standards, risks, and technologies)?
2. Are the proposed changes sufficient and appropriate? Are there other elements that should be considered under each area?
3. Do the proposed changes support different use cases in various sectors, types, and sizes of organizations (and with varied capabilities, resources, and technologies)?
4. Are there additional changes not covered here that should be considered?
5. For those using CSF 1.1, would the proposed changes affect continued adoption of the Framework, and how so?
6. For those not using the Framework, would the proposed changes affect the potential use of the Framework?

Feedback and comments should be directed to cyberframework@nist.gov by March 3, 2023. All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, or confidential business information should not be included. Comments with inappropriate language will not be considered. The changes proposed in this paper will also be discussed at the upcoming second CSF 2.0 virtual workshop on February 15, 2023, and during CSF 2.0 in-person working sessions on February 22-23, 2023. Contact cyberframework@nist.gov if you would like NIST to consider participating at a conference, webinar, or informal roundtable to discuss the CSF update and this paper.

After reviewing feedback on this concept paper and considering insights gained through the workshops, NIST intends to publish the draft Cybersecurity Framework 2.0 in the coming months for a 90-day public review.

Clearwater

Time to Act

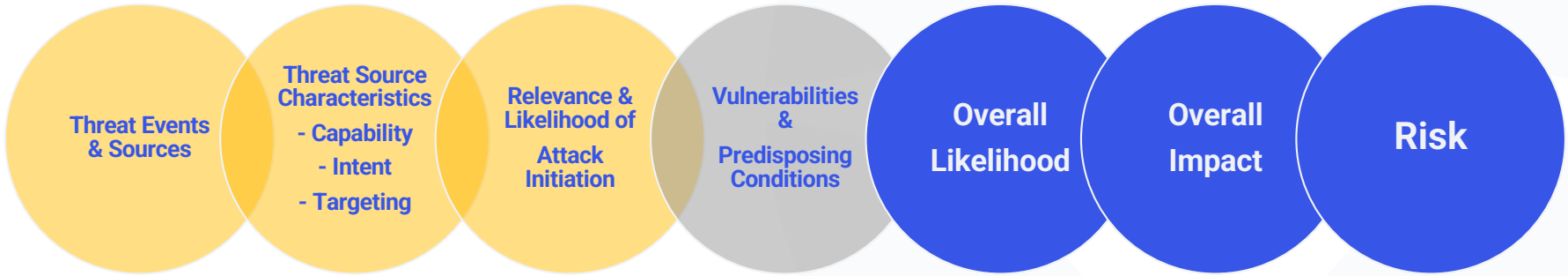
Planning: Understand the changes and enhancements with NIST CSF 2.0

Preparation: Update your security strategy to achieve a new target profile

Assumption: New evaluation criteria is required to determine the performance of your security program

Insights

- We must continue to advance information security to achieve and maintain resilience



Know your Adversary Assess the Security Program Determine your Risk

Clearwater

Framework Overview

NIST CSF 2.0

Today: NIST Cybersecurity Framework v1.1

Function	Description	Category
Identify (ID)	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	• Asset Management ID.AM • Business Environment ID.BE • Governance ID.GV • Risk Assessment ID.RA • Risk Management ID.RM • Supply Chain Risk ID.SC
Protect (PR)	Develop and implement appropriate safeguards to ensure delivery of critical services	• Identify Management, Authentication, and Access Control PR.AC • Awareness & Training PR.AT • Data Security PR.DS • Information Protection Processes and Procedures PR.IP • Maintenance PR.MA • Protective Technology PR.PT
Detect (DE)	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	• Anomalies and Events DE.AE • Security Continuous Monitoring DE.CM • Detection Processes and Procedures DE.DP
Respond (RS)	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	• Response Planning RS.RP • Communications RS.CO • Analysis RS.AN • Mitigation RS.MI • Improvements RA.IM
Recover (RC)	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	• Recovery Planning RC.RP • Improvements RC.IM • Communications RC.CO

Tomorrow: NIST Cybersecurity Framework v2.0

Function	Description	Category
Govern (GV)	Establish and monitor organization risk management strategy, expectations, and policy.	• **Organizational Context GV.OC** • Risk Management Strategy (GV.RM) • Roles and Responsibilities (GV.RR) • Policies and Procedures (GV.PO)
Identify (ID)	Determine the current cybersecurity risk to the organization.	• Asset Management ID.AM • Risk Assessment (ID.RA) • Supply Chain Risk ID.SC • Improvements ID.IM
Protect (PR)	Use safeguards to sufficiently mitigate and reduce cybersecurity risk.	• Identify Management, Authentication, and Access Control PR.AA • Awareness & Training PR.AT • Data Security PR.DS • Protective Technology PR.PT • **Platform Security (PR.PS)** • **Technology Infrastructure Resilience (PR.IR)**
Detect (DE)	Find and analyze possible cybersecurity attacks and compromises.	• Adverse Event Analysis (DE.AE) • Continuous Monitoring DE.CM
Respond (RS)	Take action regarding a detected cybersecurity incident.	• Incident Management (RS.MA) • Incident Analysis (RS.AN) • Incident Response Reporting and Communication (RS.CO) • Incident Mitigation (RS.MI)
Recover (RC)	Restore assets and operations that were impacted by a cybersecurity incident.	• Incident Recovery Plan Execution (RC.RP) • Incident Recovery Communication (RC.CO)

Overlay

Function	V1.1 Category	V2.0 Category
Govern (GV)		• **Organizational Context GV.OC** • **Risk Management Strategy (GV.RM)** • **Roles and Responsibilities (GV.RR)** • **Policies and Procedures (GV.PO)**
Identify (ID)	• Asset Management ID.AM • Business Environment ID.BE • Governance ID.GV • Risk Assessment ID.RA • Risk Management ID.RM • Supply Chain Risk ID.SC	• **Asset Management ID.AM** • **Risk Assessment (ID.RA)** • **Supply Chain Risk ID.SC** • **Improvements ID.IM**
Protect (PR)	• Identify Management, Authentication, and Access Control PR.AC • Awareness & Training PR.AT • Data Security PR.DS • Information Protection Processes and Procedures PR.IP • Maintenance PR.MA • Protective Technology PR.PT	• **Identify Management, Authentication, and Access Control PR.AA** • **Awareness & Training PR.AT** • **Data Security PR.DS** • **Protective Technology PR.PT** • **Platform Security (PR.PS)** • **Technology Infrastructure Resilience (PR.IR)**
Detect (DE)	• Anomalies and Events DE.AE • Security Continuous Monitoring DE.CM • Detection Processes and Procedures DE.DP	• **Adverse Event Analysis (DE.AE)** • **Continuous Monitoring DE.CM**
Respond (RS)	• Response Planning RS.RP • Communications RS.CO • Analysis RS.AN • Mitigation RS.MI • Improvements RA.IM	• **Incident Management (RS.MA)** • **Incident Analysis (RS.AN)** • **Incident Response Reporting and Communication (RS.CO)** • **Incident Mitigation (RS.MI)**
Recover (RC)	• Recovery Planning RC.RP • Improvements RC.IM • Communications RC.CO	• **Incident Recovery Plan Execution (RC.RP)** • **Incident Recovery Communication (RC.CO)**

Govern (GV)

Establish and monitor organization risk management strategy, expectations, and policy.

Category	Description	Sub-Cat	Description
Organizational Context (GV.OC)	**The organization's risk context, including mission, mission priorities, stakeholders, objectives, and direction, is understood**	GV.OC-01	**Organizational mission is understood in order to prioritize cybersecurity risk management**
		GV.OC-02	Internal and external stakeholders, and their expectations regarding cybersecurity risk management, are determined
		GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
		GV.OC-04	**Critical objectives, capabilities, and services that stakeholders expect are determined and communicated**
Risk Management Strategy (GV.RM)	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established and used to support operational risk decisions	GV.RM-01	Cybersecurity risk management objectives are established and agreed to by organizational stakeholders
		GV.RM-02	Cybersecurity supply chain risk management strategy is established, agreed to by organizational stakeholders, and managed
		GV.RM-03	**Risk appetite and risk tolerance statements are determined and communicated based on the organization's business environment**
		GV.RM-04	**Cybersecurity risk management is considered part of enterprise risk management**
		GV.RM-05	**Strategic direction describing appropriate risk response options, including cybersecurity risk transfer mechanisms (e.g., insurance, outsourcing), investment in mitigations, and risk acceptance is established and communicated**
		GV.RM-06	Responsibility and accountability are determined and communicated for ensuring that the risk management strategy and program are resourced, implemented, assessed, and maintained

Govern (GV)

Establish and monitor organization risk management strategy, expectations, and policy.

Category	Description	Sub-Cat	Description
Roles and Responsibilities (GV.RR)	Cybersecurity roles and responsibilities are coordinated and aligned with all internal and external stakeholders to enable accountability, performance assessment, and continuous improvement	GV.RR-01	**Organizational leadership takes responsibility for decisions associated with cybersecurity risks and establishes a culture that is risk-aware, behaves in an ethical manner, and promotes continuous improvement**
		GV.RR-02	Roles and responsibilities related to cybersecurity risk management are established and communicated
		GV.RR-03	Roles and responsibilities for customers, partners, and other third-party stakeholders are established and communicated
		GV.RR-04	Roles and responsibilities for suppliers are established, documented in contractual language, and communicated
		GV.RR-05	Lines of communication across the organization are established for cybersecurity risks, including supply chain risks
		GV.RR-06	Resourcing and authorities for cybersecurity are decided commensurate with risk strategy, roles, and policies
		GV.RR-07	**Cybersecurity is included in human resources practices**
Policies and Procedures (GV.PO)	Organizational cybersecurity policies, processes, and procedures are established and communicated	GV.PO-01	Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, risk management strategy, and priorities and are communicated
		GV.PO-02	**The same policies used internally are applied to suppliers**
		GV.PO-03	Policies and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and organizational mission

Identify (ID)

Determine the current cybersecurity risk to the organization.

Category	Description	Sub-Cat	Description
Asset Management ID.AM	Assets (e.g., data, devices, software, systems, facilities, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	ID.AM-01	Inventories of physical devices managed by the organization are maintained
		ID.AM-02	Inventories of software and services managed by the organization are maintained
		ID.AM-03	Representations of the organization's authorized network communication and network data flows are maintained
		ID.AM-04	Inventories of external assets and suppliers are maintained
		ID.AM-05	Assets are prioritized based on classification, criticality, resources, and organizational value
		ID.AM-06	**Sensitive data and corresponding metadata are inventoried and tracked**
		ID.AM-07	**Systems, devices, and software are managed throughout their life cycle, including pre-deployment checks, preventive maintenance, transfers, end-of- life, and disposition**
Risk Assessment (ID.RA)	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established and used to support operational risk decisions	ID.RM-01	Cybersecurity risk management objectives are established and agreed to by organizational stakeholders
		ID.RM-02	Cybersecurity supply chain risk management strategy is established, agreed to by organizational stakeholders, and managed
		ID.RM-03	Risk appetite and risk tolerance statements are determined and communicated based on the organization's business environment
		ID.RM-04	Cybersecurity risk management is considered part of enterprise risk management
		ID.RM-05	Strategic direction describing appropriate risk response options, including cybersecurity risk transfer mechanisms (e.g., insurance, outsourcing), investment in mitigations, and risk acceptance is established and communicated
		ID.RM-06	Responsibility and accountability are determined and communicated for ensuring that the risk management strategy and program are resourced, implemented, assessed, and maintained

Identify (ID) Determine the current cybersecurity risk to the organization.

Category	Description	Sub-Cat	Description
Supply Chain Risk Management (ID.SC)	The organization's supply chain risks are identified, assessed, and managed consistent with the organization's priorities, constraints, risk tolerances, and assumptions	ID.SC-01	**Cybersecurity requirements are integrated into contracts with suppliers and third-party partners**
		ID.SC-02	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
		ID.SC-03	**Supplier termination and transition processes include security considerations**
Improvement (ID.IM)	Improvements to organizational cybersecurity risk management processes and activities are identified	ID.RM-01	**Continuous evaluation, including through reviews, audits, and assessments (including self-assessments), is applied to identify opportunities for improvement across all Framework Functions**
		ID.RM-02	**Security tests and exercises, including in coordination with suppliers and third-party providers, are carried out to identify improvements**
		ID.RM-03	Improvements for processes and activities across all Framework Functions are identified based on lessons learned

Protect (PR) Use safeguards to sufficiently mitigate and reduce cybersecurity risk.

Category	Description	Sub-Cat	Description
Identity Management, Authentication, and Access Control (PR.AA)	Access to physical and logical assets is limited to authorized users, processes, and devices, and is managed commensurate with the assessed risk of unauthorized access	PR.AA-01	Identities and credentials for authorized users, processes, and devices are managed by the organization
		PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions
		PR.AA-03	Users, processes, and devices are authenticated
		PR.AA-04	**Federated assertions are generated, protected, conveyed, and verified**
		PR.AA-05	Access permissions, entitlements, and authorizations are managed and enforced, incorporating the principles of least privilege and separation of duties
		PR.AA-06	Account activities and access events are audited and monitored to enforce authorized access
		PR.AA-07	Physical access to assets is managed, monitored, and enforced
Awareness and Training (PR.AT)	The organization's personnel and third-parties are provided cybersecurity awareness and training to perform their cybersecurity-related tasks consistent with related policies, procedures, and agreements	PR.AT-01	Awareness and training are provided for users so they possess the knowledge and skills to perform relevant tasks
		PR.AT-02	Awareness and training are provided for users with elevated privileges so they possess the knowledge and skills to perform relevant tasks
		PR.AT-03	**Awareness and training are provided for third parties with cybersecurity responsibilities (e.g., suppliers, partners, customers) so they possess the knowledge and skills to perform relevant tasks**
		PR.AT-04	Awareness and training are provided to senior leaders so they possess the knowledge and skills to govern and lead a cybersecurity risk-aware culture

Protect (PR) Use safeguards to sufficiently mitigate and reduce cybersecurity risk.

Category	Description	Sub-Cat	Description
Data Security (PR.DS)	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest is protected
		PR.DS-02	The confidentiality, integrity, and availability of data-in-transit is protected
		PR.DS-03	**Data is managed throughout its life cycle, including discovery, maintenance, and destruction**
		PR.DS-04	The confidentiality, integrity, and availability of data-in-use is protected
		PR.DS-05	Backups of data are conducted, protected, maintained, and tested
Platform Security (PR.PS)	**The hardware and software (e.g., firmware, operating systems, applications) of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability**	PR.PS-01	Configuration management practices are applied (e.g., least functionality, least privilege)
		PR.PS-02	Software is patched, updated, replaced, and removed commensurate with risk
		PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk
		PR.PS-04	**Log records are generated for cybersecurity events and made available for continuous monitoring**
		PR.PS-05	Protective technologies are executed on or within platforms to stop unauthorized software execution
		PR.PS-06	Backups of platform software are conducted, protected, maintained, and tested
		PR.PS-07	Secure software development practices are integrated and their performance is monitored throughout the software development life cycle
		PR.PS-08	Supply chain security practices are integrated and their performance is monitored throughout the technology product and service life cycle

Protect (PR) Use safeguards to sufficiently mitigate and reduce cybersecurity risk.

Category	Description	Sub-Cat	Description
Technology Infrastructure Resilience (PR.IR)	**Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organization resilience**	PR.IR-01	Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) are communicated and maintained
		PR.IR-02	The organization's networks and environments are protected from unauthorized logical access and usage
		PR.IR-03	The organization's computing assets are protected from environmental threats
		PR.IR-04	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
		PR.IR-05	Adequate resource capacity (e.g., storage, power, network bandwidth, computing) to ensure availability is maintained

Detect (DE)

Find and analyze possible cybersecurity attacks and compromises.

Category	Description	Sub-Cat	Description
Adverse Event Analysis (DE.AE)	Adverse cybersecurity events are analyzed to find and characterize possible attacks and compromises, unauthorized and inappropriate activities, protection deficiencies, and other activity with a potentially negative impact on cybersecurity	DE.AE-01	Adverse events are analyzed to find possible attacks and compromises
		DE.AE-02	Information on adverse events is correlated from multiple sources
		DE.AE-03	The estimated impact and scope of adverse events is determined
		DE.AE-04	Incident alert thresholds are established
		DE.AE-05	Information on adverse events is provided to cybersecurity and incident response tools and staff
		DE.AE-06	**Contextual information (e.g., cyber threat intelligence, inventories, security advisories) is integrated into the adverse event analysis**
		DE.AE-07	Adverse cybersecurity events are categorized and potential incidents are escalated for triage
Continuous Monitoring (DE.CM)	Assets are monitored to find potential adverse cybersecurity events, including indicators of attacks and compromise, unauthorized and inappropriate activity, protection deficiencies and failures and other activity with a potentially negative impact on cybersecurity	DE.CM-01	Networks and network services are monitored to find adverse cybersecurity events
		DE.CM-02	The physical environment is monitored to find adverse cybersecurity events
		DE.CM-03	Personnel activity and technology usage are monitored to find adverse cybersecurity events
		DE.CM-04	**External service providers and the services they provide are monitored to find adverse cybersecurity events**
		DE.CM-05	**Computing hardware and software and their data are monitored to find adverse cybersecurity events**

Respond (RS)

Take action regarding a detected cybersecurity incident.

Category	Description	Sub-Cat	Description
Response Planning (RS.RP)	Responses to detected cybersecurity incidents are managed	RS.MA-01	The incident response plan is executed
		RS.MA-02	Incident reports are triaged and validated
		RS.MA-03	Incidents are categorized and prioritized
		RS.MA-04	Incidents are escalated or elevated as needed
		RS.MA-05	Criteria for initiating incident recovery defined and applied
Incident Analysis (RS.AN)	Investigation is conducted to ensure effective response and support recovery activities	RS.AN-01	Analysis is performed to determine what has taken place during an incident and the root cause of the incident
		RS.AN-02	Actions performed during an investigation are recorded and the record's integrity and provenance are preserved
		RS.AN-03	Incident data and metadata are collected and their integrity and provenance are preserved
		RS.AN-04	Incident magnitude is estimated and validated
		RS.AN-05	Incident status is tracked and validated

Recover (RC)

Restore assets and operations that were impacted by a cybersecurity incident

Category	Description	Sub-Cat	Description
Incident Recovery Plan Execution (RC.RP)	Restoration activities are planned and performed to ensure full operational availability of systems and services affected by cybersecurity incidents	RC.RP-01	The incident recovery plan is executed
		RC.RP-02	Recovery actions are determined, scoped, prioritized, and performed
		RC.RP-03	**The integrity of backups and other restoration assets is verified before using them for restoration**
		RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms
		RC.RP-05	**The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed**
		RC.RP-06	Criteria for determining the end of incident recovery are defined and applied, and incident-related documentation is completed
Incident Recovery Communication (RC.CO)	Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other computer security incident response teams, and vendors)	RC.CO-01	Public relations are managed
		RC.CO-02	Reputation is repaired after an incident
		RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders

Next Steps

Plan: Understand the changes and enhancements with NIST CSF 2.0

Prepare: Update your security strategy to achieve a new target profile

Assume: New evaluation criteria is required to determine conformance and effectiveness of the categories

Q&A

Steve Cagle
Dave Bailey
Rick Lemay

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Upcoming Events

HIMSS Healthcare Cybersecurity Forum | September 7 - 8, 2023, Boston, MA

Dykema

Dykema | July 19-21, 2023

August Cyber Briefing | August 3, 2023,12pm – 1pm (CT)

Clearwater

Clearwater

Healthcare–Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394