Check for updates

NIST Internal Report
NIST IR 8374r1 ipd

Ransomware Risk Management:

A Cybersecurity Framework 2.0 Community Profile

Initial Public Draft

Murugiah Souppaya
William C. Barker
William Fisher
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374r1.ipd

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Internal Report
NIST IR 8374r1 ipd

Ransomware Risk Management:

A Cybersecurity Framework 2.0 Community Profile

Initial Public Draft

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

William C. Barker
Dakota Consulting
Silver Spring, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374r1.ipd

January 2025

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Charles H. Romine, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication
Souppaya M, Barker WC, Fisher W, Scarfone K (2025) Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8374r1 ipd. https://doi.org/10.6028/NIST.IR.8374r1.ipd

Author ORCID iDs
Murugiah Souppaya: 0000-0002-8055-8527
William C. Barker: 0000-0002-4113-8861
William Fisher: 0009-0004-7569-5668
Karen Scarfone: 0000-0001-6334-9486

Public Comment Period
January 13, 2025 – ~~March 14~~ September 11, 2025

Submit Comments
ransomware@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8374/r1/ipd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA)

Abstract

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. This Cybersecurity Framework (CSF) 2.0 Community Profile identifies the security objectives from the NIST CSF 2.0 that support governing management of, identifying, protecting against, detecting, responding to, and recovering from ransomware events. The Profile can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to counter ransomware threats and to deal with the potential consequences of events. This Profile can be leveraged in developing a ransomware countermeasure playbook.

Keywords

Cybersecurity Framework; detect; identify; protect; ransomware; recover; respond; risk; security.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Audience

This Ransomware Community Profile is intended for any organization (including industry, government, and nonprofits) that could be subject to ransomware attacks, regardless of sector or size. As the Profile helps to prioritize efforts, it could be especially valuable for smaller and less resourced organizations.

In addition, the Profile is intended for organizations that:

- are familiar with – and may have already adopted – the CSF to help manage cybersecurity risks and want to improve their risk postures by addressing ransomware threats, or
- are not familiar with the CSF but want to implement risk management frameworks to mitigate ransomware threats. Such organizations may wish to review the CSF for additional context and guidance.

Note to Reviewers

This draft Ransomware Community Profile reflects changes due to the update from CSF 1.1 to CSF 2.0. The Ransomware Community Profile is a widely used guidance document, both domestically and internationally. NIST is currently considering a more comprehensive revision to this Profile to reflect recent ransomware policy developments and incorporate the results of collaborative activities in the ransomware prevention and response space. NIST is interested in your feedback on what guidance and content would be most valuable. Specifically, NIST is interested in answers to the following questions:

1. What elements of this Community Profile have been helpful?
2. Where could this Community Profile be improved?
3. Are supplemental documents, such as quick start guides, useful? If so, how? If not, why?
4. What type of prioritization would be most helpful? Control baselines? high/medium/low criticality? Mapping to specific organizational outcomes? Other?
5. What other ransomware resources have you or your organization used to improve your ransomware risk mitigation strategy? How have those resources been helpful?

General comments and answers to the above questions can be submitted to ransomware@nist.gov.

Additional Guidance Resources

NIST's National Cybersecurity Center of Excellence (NCCoE) has produced guidance to support ransomware threat mitigation. NIST has many other resources that, while not ransomware-specific, contain valuable information about governing management of, identifying, protecting against, detecting, responding to, and recovering from ransomware events. See the References section for a list of references and Appendix A for a more extensive list of NIST resources.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: ransomware@nist.gov

154 **Table of Contents**

1. Introduction

This Ransomware Community Profile can help organizations and individuals to manage the risk of ransomware events. That includes helping to gauge an organization's level of readiness to counter ransomware threats and to deal with the potential consequences of events. The Profile can also be used to identify opportunities for improving cybersecurity to help thwart ransomware. It prioritizes security objectives from the NIST Cybersecurity Framework (CSF) 2.0 [NIST CSWP 29] to security capabilities and measures that help to govern management of, identify, protect against, detect, respond to, and recover from ransomware events.

This Profile is a Community Profile that was developed in collaboration with industry to serve as a baseline of CSF outcomes that address shared interests and goals among multiple organizations. Individual organizations may use community profiles to create their own organizational profile, detailing the organization's current and/or target cybersecurity posture in terms of outcomes identified in the CSF. Examples of profiles can be found on the NIST CSF website along with a template for creating organizational profiles. The guidance in this report addresses best practices rather than a set of legal or regulatory requirements.

1.1 The Ransomware Challenge

Ransomware is a type of malware that encrypts an organization's data and demands payment as a condition of restoring access to that data. Ransomware can also be used to steal an organization's information and demand additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware events target the organization's data or critical infrastructure, disrupting or halting operations and posing a dilemma for management: pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or do not pay the ransom and attempt to restore operations themselves. The methods ransomware uses to gain access to an organization's information and systems are common to cyberattacks more broadly, but they are aimed at forcing a ransom to be paid. Techniques used to promulgate ransomware will continue to change as attackers constantly look for new ways to pressure their victims.

Ransomware attacks differ from other cybersecurity events where access may be surreptitiously gained to information such as intellectual property, credit card data, or personally identifiable information and later exfiltrated for monetization. Instead, ransomware threatens an immediate impact on business operations. During a ransomware event, organizations may be afforded little time to mitigate or remediate impact, restore systems, or communicate via necessary business, partner, and public relations channels. For this reason, it is especially critical that organizations be prepared. That includes educating users of cyber systems, response teams, and business decision makers about the importance of – and processes and procedures for – preventing and handling potential compromises before they occur.

Fortunately, organizations can follow recommended steps to prepare for and reduce the potential for successful ransomware attacks. This includes the following: establish, communicate and monitor ransomware risk strategy, expectations and policy; identify and

protect critical data, systems, and devices; detect ransomware events as early as possible (preferably before the ransomware is deployed); and prepare to respond to and recover from any ransomware events that do occur. There are many resources available to assist organizations in these efforts. They include information from the National Institute of Standards and Technology (NIST), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS). Additional NIST resources are listed in Appendix A.

1.2 Basic Ransomware Tips

The security capabilities and measures in this profile support a detailed approach to preventing and mitigating ransomware events. Realizing that undertaking all these measures may be beyond the reach of some, the text box below includes basic preventative steps that an organization can take now to protect against the ransomware threat. Not all these measures will apply to the situations of all organizations.

BASIC RANSOMWARE TIPS

Even without undertaking all the measures described in this Ransomware Community Profile, there are some basic preventative steps that an organization can take now to protect against and recover from the ransomware threat. These include:

1. Educate employees on avoiding ransomware infections.

- **Don't open files or click on links from unknown sources** unless you first run an antivirus scan or look at links carefully.
- **Avoid using personal websites and personal apps** – like email, chat, and social media – from work computers.
- **Don't connect personally owned devices to work networks without prior authorization.**

2. Avoid having vulnerabilities in systems that ransomware could exploit.

- **Keep relevant systems fully patched.** Run scheduled checks to identify available patches and install these as soon as feasible.
- **Employ zero trust principles in all networked systems.** Manage access to all network functions, and segment internal networks where practical to prevent malware from proliferating among potential target systems.
- **Allow installation and execution of authorized apps only.** Configure operating systems and/or third-party software to run only authorized applications. This can also be supported by adopting a policy for reviewing, then adding or removing authorized applications on an allow list.
- **Inform your technology vendors of your expectations** (e.g., in contract language) that they will apply measures that discourage ransomware attacks.

3. Quickly detect and stop ransomware attacks and infections.

- **Use malware detection software, such as antivirus software at all times.** Set it to automatically scan emails and flash drives.
- **Continuously monitor** directory services (and other primary user stores) for indicators of compromise or active attack.

- **Block access to untrusted web resources.** Use products or services that block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity. This includes using products and services that provide integrity protection for the domain component of addresses (e.g., hacker@poser.com).

4. Make it harder for ransomware to spread.

- **Use standard user accounts** with multi-factor authentication versus accounts with administrative privileges whenever possible.
- **Introduce authentication delays or configure automatic account lockout** as a defense against automated attempts to guess passwords.
- **Assign and manage credential authorization** for all enterprise assets and software and periodically verify that each account has only the necessary access following the principle of least privilege.
- **Store data in an immutable format** (so that the database does not automatically overwrite older data when new data is made available).
- **Allow external access to internal network resources via secure virtual private network (VPN) connections only.**

5. Make it easier to recover stored information from a future ransomware event.

- **Make an incident recovery plan.** Develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization, and business continuity plans for those critical services.
- **Back up data, secure backups, and test restoration.** Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.
- **Keep your contacts.** Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.

2. The Ransomware Community Profile

The Ransomware Community Profile aligns organizations' ransomware prevention and mitigation requirements, objectives, risk appetite, and resources with the elements of the CSF. It should help organizations to identify and prioritize opportunities for improving their security and resilience against ransomware attacks. Organizations can use this document as a guide for profiling the state of their own readiness. Doing so will assist them to determine their current "organizational profile" or state and set a "target organizational profile" to identify gaps.

The table below identifies Categories and Subcategories from CSF 2.0 that are particularly relevant to mitigating ransomware risk. The first two columns list these Categories and Subcategories which organizations may use as priority target outcomes for ransomware risk management programs. All subcategories included in the table are priority objectives, but the third column highlights subcategories that have been identified as *Priority 1* or *Priority 2*. The fourth column briefly explains how each Subcategory helps to govern management of, identify, protect against, detect, respond to, and recover from ransomware events and details a rationale for subcategories' *Priority 1* assignments. It is important to note that subcategories assigned *Priority 2* rather than *Priority 1* are still highly important to organizations' ransomware-specific defense posture.

Organizations are encouraged to include the full set of CSF 2.0 Subcategories for their cybersecurity risk management programs. The selection of subcategories highlighted in this document are specific to ransomware risks.

NIST and other organizations have produced a suite of online resources that help organizations understand, adopt, and use the CSF, including Informative References, Implementation Examples, and Quick Start Guides.

The six Cybersecurity Framework Functions used to organize the Categories are:

- **GOVERN (GV)** — *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
- **IDENTIFY (ID)** — *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures,

and practices that support cybersecurity risk management to inform efforts under all six Functions.

- **PROTECT (PR)** — *Safeguards to manage the organization's cybersecurity risks are used.* Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
- **DETECT (DE)** — *Possible cybersecurity attacks and compromises are found and analyzed.* DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
- **RESPOND (RS)** — *Actions regarding a detected cybersecurity incident are taken.* RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- **RECOVER (RC)** — *Assets and operations affected by a cybersecurity incident are restored.* RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

The CSF 2.0 outcomes included in the table also map to controls, requirements, and recommendations of other security standards and guidance documents. Examples include NIST's Special Publication 800-53; ISO/IEC information, security, cybersecurity, and privacy protection standards, and industry consensus standards. The Cybersecurity and Privacy Reference Tool (CPRT) highlights the reference data from NIST publications without the constraints of PDF files. This enables stakeholders to interactively browse, search, and export the data in a structured format that is human- and machine-consumable. For example, you can use the search tool to locate reference data in each publication and then download the reference data for each publication in MS Excel or JSON. The Online Informative Reference Catalog contains the reference data, including Informative References and Derived Relationship Mappings (DRMs), for the National Online Informative References (OLIR) Program.

286 **Table 1. Ransomware Community Profile**

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	**GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management	2	Priorities for organizational mission, objectives, and activities are established and communicated. Understanding priorities for organizational objectives and activities is needed to support contingency planning for future ransomware events and emergency response and recovery actions. For example, the most critical enterprise information and operational activities or functions might be given the highest priority for backup as well as for access management.
Organizational Context (GV.OC)	**GV.OC-02:** Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	1	Understanding the needs and expectations of internal and external stakeholders with respect to cybersecurity risk management is needed to support contingency planning for future ransomware events and emergency response and recovery actions (e.g., notification requirements). The priority for this outcome is designated *Priority 1* because of both the importance of everyone understanding the consequences of a successful ransomware attack, and the need to understand the impact of the attack on specific internal and external stakeholders.
Organizational Context (GV.OC)	**GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	2	Understanding legal and regulatory requirements regarding cybersecurity and privacy is necessary for organizational cybersecurity policy development and for establishing priorities in contingency planning for responses to and recovery from future ransomware events.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	**GV.RM-03:** Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	2	Ransomware risks must be factored into organizational risk management governance to support establishment of adequate organizational cybersecurity policies.
Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	**GV.RR-02:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	1	Because ransomware events often result in the immediate loss of business functionality, organizations face extreme pressure to recover business functions quickly. Effective ransomware mitigation and response requires everyone in the organization understand their role, responsibility, and authority prior to a ransomware event. Because this is critical to mitigating ransomware impact and restoring business function, this outcome is designated *Priority 1*.
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	**GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	1	Many ransomware events are enabled by some member of the workforce or a third-party stakeholder taking an intentional or inadvertent action that enables infiltration by criminals or other unauthorized parties. It's important to understand roles and responsibilities for preventing ransomware infections and the associated responsibilities with response and recovery actions. For this reason, the outcome is designated *Priority 1*.
Cybersecurity Supply Chain Risk Management (GV.SC)	**GV.SC-08:** Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	2	Ransomware contingency planning should be coordinated with suppliers and third-party providers, and planning should include provision for testing of planned activities.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, 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-02:** Inventories of software, services, and systems managed by the organization are maintained	1	It is important to update your software as soon as practical after updates become available to remove vulnerabilities that attackers can take advantage of to infiltrate your systems using ransomware. Also, some software utilities and applications contain known vulnerabilities used for intrusion. Software inventories may track elements such as software name and version, devices where it's currently installed, last patch date, and current known vulnerabilities. This information supports scheduling updates and removing vulnerable utilities and applications. Because of the importance of timely updates in eliminating vulnerabilities that ransomware actors exploit, this outcome is designated *Priority 1*.
Asset Management (ID.AM)	**ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained	2	Understanding organizational communications and data flows is needed as preparation for responding to future ransomware events. In addition to enabling assignment of responsibilities, knowing the connections and flows helps to enumerate what information or processes are at risk based on the identified criminal infiltration. Cataloging connections to external information systems is important for planning communications to partners and possible actions to temporarily disconnect from external systems in response to ransomware events. Identifying these connections will also help organizations plan security control implementation and identity areas where controls may be shared with third parties. Note that ransomware attacks can disable common communication channels (e.g., email)> It is essential that planning include means for communication with staff and partners in the event of such attacks.
Asset Management (ID.AM)	**ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission	2	Prioritization of data and software based on classification, criticality, and business value is essential to understanding the true scope and impact of ransomware events and is an important factor in both contingency planning for future ransomware events, and emergency responses and recovery actions.
Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	**ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded	2	Identifying and documenting the vulnerabilities of organizational assets supports development and prioritization of planning to mitigate or eliminate those vulnerabilities as well as contingency planning for evaluation of and responses to future ransomware events.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Risk Assessment (ID.RA)	**ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	1	Understanding the business impacts of potential ransomware events is needed to support cybersecurity cost-benefit analyses as well as to establish priorities for activities included in ransomware contingency plans for response and recovery. Understanding the potential business impacts also supports emergency response decisions in the event of a ransomware attack. Because understanding the potential impact of a successful ransomware attack is a critical factor in determining the response to criminal demands, this outcome is designated *Priority 1*.
Risk Assessment (ID.RA)	**ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated	2	The expense associated with response to and recovery from ransomware events is materially affected by the effectiveness of contingency planning of responses to projected risks.
Risk Assessment (ID.RA)	**ID.RA-09:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use	2	Software of unknown or unreliable provenance can contain malware or otherwise be subject to exploitation by bad actors.
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	**ID.IM-04:** Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	2	Response and recovery plans should include response to and recovery from future ransomware events. Ransomware response and recovery plans should be tested periodically to ensure that risk and response assumptions and processes are current with respect to evolving ransomware threats.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	**PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization	1	Because ransomware attacks often start with credential compromise, proper credential management is an essential mitigation. The type of credential and how credentials are issued, managed, revoked and recovered are critical considerations for preventing credential compromise that could lead to ransomware events. For this reason, this outcome is designated *Priority 1*.
Identity Management, Authentication, and Access Control (PR.AA)	**PR.AA-03:** Users, services, and hardware are authenticated	2	Most ransomware attacks are conducted through network connections, and because social engineering-based compromise of passwords is a major source of compromise, authentication of identities using phishing-resistant multi-factor authentication is strongly recommended.
Identity Management, Authentication, and Access Control (PR.AA)	**PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	2	Many ransomware intrusions occur through the compromise of user credentials or invoking processes that should not be authorized to have privileged access to the process that is being infiltrated.
Identity Management, Authentication, and Access Control (PR.AA)	**PR.AA-06:** Physical access to assets is managed, monitored, and enforced commensurate with risk	2	Although most ransomware attacks are conducted remotely, managing and protecting physical access does protect against insider attacks. This includes protection against others, including family members, accessing physical devices and intentionally or inadvertently degrading the logical access protections associated with the devices.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks	**PR.AT-01:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	1	Most ransomware attacks are made possible by users who engage in unsafe practices, administrators who implement insecure configurations, or developers who have insufficient security training. For this reason, this CSF outcome is designated *Priority 1*.
Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-11:** Backups of data are created, protected, maintained, and tested	1	Regular backups that are maintained and tested are essential to timely and relatively painless recovery from ransomware events. Backups should have a copy stored offline or otherwise in a manner that prevents access to them by the attacker or compromise by ransomware. Because this CSF outcome is so important to mitigating the effects of ransomware attacks, this outcome is designated *Priority 1*.
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services 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 established and applied	2	Proper configuration change processes can help to enforce timely security updates to software, maintain necessary security configuration settings, and discourage replacement of code with products that contain malware or don't satisfy access management policies. This CSF outcome reduces an attacker's opportunities to exploit system vulnerabilities, thus protecting against ransomware attacks.
Platform Security (PR.PS)	**PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk	1	Old versions of software may contain vulnerabilities of which ransomware actors are aware and can exploit. Software updates should be promptly installed, and software that is no longer supported should be replaced. Because is a commonly exploited vulnerability, this outcome is designated *Priority 1*.
Platform Security (PR.PS)	**PR.PS-04:** Log records are generated and made available for continuous monitoring	2	Availability of audit/log records can assist forensics in support of recovery and response processes.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Platform Security (PR.PS)	**PR.PS.05:** Installation and execution of unauthorized software are prevented	2	Software of unknown or unreliable provenance can contain malware or other vulnerabilities that can be exploited by a ransomware actor. This objective includes employing protection mechanisms such as technologies that prevent malware installation, use allowlisting/denylisting protections for executables, and block access to known-malicious domains.
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage	1	Most ransomware attacks are executed remotely. Protection of network connections can include processes as simple as password protection of Wi-Fi connections to personal computers and firewalls. In general, use of zero-trust network principles is encouraged. Because remote attacks are so prevalent, this outcome is designated *Priority 1*.
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-01:** Networks and network services are monitored to find potentially adverse events	2	Network monitoring may sometimes detect intrusions before malicious code can be inserted or large volumes of information exfiltrated.
Continuous Monitoring (DE.CM)	**DE.CM-03:** Personnel activity and technology usage are monitored to find potentially adverse events	2	Monitoring personnel activity can sometimes detect insider threats or insecure staff practices, and thwart potential ransomware events. Monitoring can also be used to find unusual patterns of usage, like someone logging on from another country.
Continuous Monitoring (DE.CM):	**DE.CM-06:** External service provider activities and services are monitored to find potentially adverse events	2	Ransomware can be introduced intentionally or inadvertently by external service providers, especially where remote maintenance takes place. Monitoring can detect exploitable vulnerabilities before ransomware actors take advantage of them.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Continuous Monitoring (DE.CM):	**DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	2	Often malicious code is not immediately executed. There may be time between its insertion and its activation to detect it before the ransomware attack is executed.
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	**DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities	1	Identifying the cause of potentially adverse behaviors can prevent or mitigate attacks. For example, receipt of data from unknown sources or sudden slowing of response times may indicate attempts to insert malware or exfiltrate information. Unknown mail headers can be clicked on to provide additional sender information and reveal suspicious senders. Terminating connections can abort exfiltration. Data center operations can undertake forensics activities to ascertain the nature and extent of attacks. The importance of recognizing and understanding anomalies is such that this outcome is designated *Priority 1*.
Adverse Event Analysis (DE.AE)	**DE.AE-04:** The estimated impact and scope of adverse events are understood	2	Determining the impact of events can inform response and recovery priorities to include supporting a cost-benefit analysis when deciding if a ransom should be paid.
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed	**RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared	2	Immediate execution of the response plan is necessary to stop any continuing exfiltration of data, stem the spread of an infection to other systems and networks, and initiate pre-emptive messaging.
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	**RS.CO-02:** Internal and external stakeholders are notified of incidents	2	Response to ransomware events include both technical and business responses. An efficient response requires all parties to understand their role.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Incident Response Reporting and Communication (RS.CO)	**RS.CO-03:** Information is shared with designated internal and external stakeholders	2	Information sharing priorities include stemming the spread of an infection to other systems and networks as well as pre-emptive messaging. Information sharing may also yield forensic benefits and reduce profitability of ransomware attacks.
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	**RS.MI-01:** Incidents are contained	1	Immediate action must be taken to minimize the damage to systems and data, to prevent the spread of infection to other systems and networks, and to minimize the impact on the mission or business. Containment of the effects of the incident is of such importance that this outcome is designated *Priority 1*.
Incident Mitigation (RS.MI):	**RS.MI-02:** Incidents are eradicated	2	This is necessary to minimize the probability of future successful ransomware attacks and to restore confidence among stakeholders.
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed	**RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared	2	Immediate execution of the response plan is necessary to stop any continuing exfiltration of data, stem the spread of an infection to other systems and networks, and initiate pre-emptive messaging.
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	**RS.CO-02:** Internal and external stakeholders are notified of incidents	2	Response to ransomware events include both technical and business responses. An efficient response requires all parties to understand their role.
Incident Response Reporting and Communication (RS.CO)	**RS.CO-03:** Information is shared with designated internal and external stakeholders	2	Information sharing priorities include stemming the spread of an infection to other systems and networks as well as pre-emptive messaging. Information sharing may also yield forensic benefits and reduce profitability of ransomware attacks.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	**RS.MI-01:** Incidents are contained	1	Immediate action must be taken to minimize the damage to systems and data, to prevent the spread of infection to other systems and networks, and to minimize the impact on the mission or business. Containment of the effects of the incident is of such importance that this outcome is designated *Priority 1*.
Incident Mitigation (RS.MI)	**RS.MI-02:** Incidents are eradicated	2	This is necessary to minimize the probability of future successful ransomware attacks and to restore confidence among stakeholders.
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process	2	Immediate initiation of the recovery plan can cut losses.
Incident Recovery Plan Execution (RC.RP)	**RC.RP-02:** Recovery actions are selected, scoped, prioritized, and performed	2	Recovery actions are necessary to restore mission effectiveness and business reputation.
Incident Recovery Plan Execution (RC.RP)	**RC.RP-03:** The integrity of backups and other restoration assets is verified before using them for restoration	1	It is important to verify the integrity of backups to ensure their efficacy for use in recovering from a ransomware event. Because restoring from backups is critical to recovery, this outcome is designated *Priority 1*.
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties	**RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	2	This is necessary to minimize the business impact and to restore confidence among stakeholders.

CSF 2.0 Category	CSF 2.0 Outcome	Priority	Ransomware Application
Incident Recovery Communication (RC.CO)	**RC.CO-04:** Public updates on incident recovery are shared using approved methods and messaging	2	This helps minimize the business impact and restore confidence among stakeholders.

Appendix A. Additional NIST Ransomware Resources

In addition to other resources cited in this document, NIST's National Cybersecurity Center of Excellence (NCCoE) has produced additional guidance to support ransomware threat mitigation. These include:

- NIST Special Publication (SP) 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* addresses how an organization can handle an attack when it occurs and what capabilities it needs to have in place to detect and respond to destructive events. Available at https://csrc.nist.gov/pubs/sp/1800/26/final.
- NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* addresses how an organization can work before an attack to identify its assets and potential vulnerabilities and remedy the discovered vulnerabilities to protect these assets. Available at https://csrc.nist.gov/pubs/sp/1800/25/final.
- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events* addresses approaches for recovery should a data integrity attack be successful. Available at https://csrc.nist.gov/pubs/sp/1800/11/final.
- Protecting Data from Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain, and Test Backup Files is a guide to help managed service providers (MSPs) improve their recovery from ransomware attacks. Available at https://csrc.nist.gov/pubs/other/2020/04/24/protecting-data-from-ransomware-and-other-data-los/final.

NIST has many other resources that, while not ransomware-specific, contain valuable information about identifying, protecting against, detecting, responding to, and recovering from ransomware events. Several are highlighted below. For a more complete list of resources, visit NIST's Ransomware Protection and Response site at https://csrc.nist.gov/ransomware.

- Improving the security of telework, remote access, and bring-your-own-device (BYOD) technologies:
  - SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* available at https://csrc.nist.gov/pubs/sp/800/46/r2/final
- Patching software to eliminate vulnerabilities:
  - SP 800-40 Revision 4, *Guide to Enterprise Patch Management Technologies* available at https://csrc.nist.gov/pubs/sp/800/40/r4/final
- Implementing a zero trust architecture to mitigate ransomware threats:
  - SP 800-207, *Zero Trust Architecture* available at https://csrc.nist.gov/pubs/sp/800/207/final
  - SP 1800-28*, Data Confidentiality: Identifying and Protecting Assets Against Data Breaches* available at https://csrc.nist.gov/pubs/sp/1800/28/final

325 - SP 1800-29, Data Confidentiality: Detect, Respond to, and Recover from Data
326 Breaches available at https://csrc.nist.gov/pubs/sp/1800/29/final
327 - SP 1800-35, *Implementing a Zero Trust Architecture* (DRAFT) available at
328 https://csrc.nist.gov/pubs/sp/1800/35/3prd
329 - IR 8496, *Data Classification Concepts and Considerations for Improving Data*
330 *Protection* (DRAFT) available at https://csrc.nist.gov/pubs/ir/8496/ipd

331 • Finding low-level guidance on securely configuring software to eliminate vulnerabilities:

332 - SP 800-70 Revision 4, *National Checklist Program for IT Products: Guidelines for*
333 *Checklist Users and Developers* available at
334 https://csrc.nist.gov/pubs/sp/800/70/r4/final