Preliminary Draft NISTIR 8374

Cybersecurity Framework Profile for Ransomware Risk Management

William C. Barker
Karen Scarfone
William Fisher
Murugiah Souppaya

This is Preliminary Draft publication.
For additional details, see the Note to Reviewers on page ii.

National Institute of Standards and Technology
U.S. Department of Commerce

Preliminary Draft NISTIR 8374

Cybersecurity Framework Profile for Ransomware Risk Management

William C. Barker
Dakota Consulting
Silver Spring, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

June 2021

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

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8374
22 pages (June 2021)

Public comment period: *June 9, 2021* through *July 9, 2021*

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

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

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.

Abstract

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, 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 Ransomware Profile identifies the Cybersecurity Framework Version 1.1 security objectives that support preventing, 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.

Keywords

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

Acknowledgments

The authors wish to thank all individuals and organizations that contributed to the creation of this document.

Note to Reviewers

NIST is adopting an agile and iterative methodology to publish this content. The content is being made available as soon as possible, rather than delaying release until all the elements are completed. This is a preliminary draft. There will be at least one additional public comment period for this.

Any updates for this document that are not yet published in an errata update or revision—including additional issues and corrections—will be posted as they are identified. See the NIST Interagency or Internal Report (NISTIR) 8374 publication details page for more information.

55 **Table of Contents**

62

1 Introduction

The Ransomware Profile defined in this report maps security objectives from the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [1] (also known as the Cybersecurity Framework) to security capabilities and measures that support preventing, 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 mitigate ransomware threats and to react to the potential impact of events. The profile can also be used to identify opportunities for improving cybersecurity to help thwart ransomware.

1.1 The Ransomware Challenge

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, 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. Ransomware disrupts or halts an organization's operations and poses 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 restore operations themselves. The methods used 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. Ransomware attacks target the organization's data.

Fortunately, organizations can follow recommended steps to prepare for and reduce the potential for successful ransomware attacks. This includes identifying and protecting critical data, systems, and devices from ransomware, and preparing to respond to any ransomware attacks that succeed. 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).

The security capabilities and measures provided in this profile support a detailed approach to preventing and mitigating ransomware events. Even without undertaking all of these measures, there are some basic preventative steps that an organization can take now to protect against the ransomware threat. These include:

- **Use antivirus software at all times.** Set your software to automatically scan emails and flash drives.
- **Keep computers fully patched.** Run scheduled checks to keep everything up-to-date.
- **Block access to ransomware sites.** Use security products or services that block access to known ransomware sites.
- **Allow only authorized apps.** Configure operating systems or use third-party software to allow only authorized applications on computers.
- **Restrict personally owned devices** on work networks.
- **Use standard user accounts** versus accounts with administrative privileges whenever possible.

- **Avoid using personal apps**—like email, chat, and social media—from work computers.
- **Beware of unknown sources.** Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.

Steps that organizations can take now to help recover from a future ransomware event include:

- **Make an incident recovery plan.** Develop and implement an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan.
- **Backup and restore.** 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.

1.2 Audience

The Ransomware Profile is intended for a general audience and is broadly applicable to organizations that:

- have already adopted the NIST Cybersecurity Framework to help identify, assess, and manage cybersecurity risks;
- are familiar with the Cybersecurity Framework and want to improve their risk postures; or
- are unfamiliar with the Cybersecurity Framework but need to implement risk management frameworks to meet ransomware threats.

1.3 Additional Resources

NIST's National Cybersecurity Center of Excellence (NCCoE) has produced additional reference materials intended to support ransomware threat mitigation. These references 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.
- 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.
- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events* addresses approaches for recovery should a data integrity attack be successful.
- *Protecting Data from Ransomware and Other Data Loss Events* is a guide for managed service providers to conduct, maintain, and test backup files that are critical to recovering from ransomware attacks.

NIST has many other resources that, while not ransomware-specific, contain valuable information about preventing, preparing for, detecting, and responding and recovering from ransomware events. Several of these resources are highlighted below. For the 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:
  - Telework: Working Anytime, Anywhere project
  - NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- **Patching software** to eliminate vulnerabilities:
  - NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*
  - Critical Cybersecurity Hygiene: Patching the Enterprise project
- **Using application control technology** to prevent ransomware execution:
  - NIST SP 800-167, *Guide to Application Whitelisting*
- Finding low-level guidance on **securely configuring software** to eliminate vulnerabilities:
  - National Checklist Program
- Getting the latest **information on known vulnerabilities**:
  - National Vulnerability Database
- **Planning for** cybersecurity event **recovery**:
  - NIST SP 800-184, *Guide for Cybersecurity Event Recovery*
- **Contingency planning for restoring operations** after a disruption caused by ransomware:
  - NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
- **Handling ransomware** and other malware **incidents**:
  - NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- **Handling** cybersecurity **incidents** in general:
  - NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*

2 The Ransomware Profile

The Ransomware Profile aligns organizations' ransomware prevention and mitigation requirements, objectives, risk appetite, and resources with the elements of the Cybersecurity Framework. The purpose of the profile is to help organizations identify and prioritize opportunities for improving their ransomware resistance. Organizations can use this document as a guide for profiling the state of their own readiness. For example, they can determine their current state and set a target profile to identify gaps to achieve their goal.

Table 1 defines the Ransomware Profile. The first two columns of the table list the relevant Categories and Subcategories from the Cybersecurity Framework. The third column briefly explains how each of the listed Subcategories supports preventing, responding to, and recovering from ransomware events.

The second column of Table 1 also cites relevant requirements from two of the informative references included in the Cybersecurity Framework: International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements* [2] and NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* [3]. Additional informative references may be included in subsequent versions of this report.

The Cybersecurity Framework lists additional Informative References for each Subcategory. Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each subcategory. The Informative References in the Cybersecurity Framework are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Cybersecurity Framework Functions that are used to organize the Categories are:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

- **Recover** – 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. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Table 1: Ransomware Profile

Category	Subcategory and Selected Informative References	Ransomware Application
Identify		
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities 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-2:** Software platforms and applications within the organization are inventoried **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 5** CM-8, PM-5	Software inventories may track information 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 that ransomware could exploit.
	ID.AM-3: Organizational communication and data flows are mapped **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 5** AC-4, CA-3, CA-9, PL-8	This helps to enumerate what information or processes are at risk, should the attackers move laterally within an environment.
	ID.AM-4: External information systems are catalogued **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 5** AC-20, SA-9	This 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 identify areas where controls may be shared with third parties.
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 5** CP-2, RA-2, RA-9, SC-6	This is essential to understanding the true scope and impact of ransomware events, and is an important factor in contingency planning for future ransomware events, emergency responses, and recovery actions. This will help prioritize the response and recovery activities.

Category	Subcategory and Selected Informative References	Ransomware Application
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 5** CP-2, PS-7, PM-11	It's important that everyone in the organization understand their roles and responsibilities for preventing ransomware events and, if applicable, also for responding to and recovering from ransomware events.
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated **NIST SP 800-53 Rev. 5** PM-11, SA-14	This helps operations and incident responders with prioritizing resources. This supports contingency planning for future ransomware events, emergency responses, and recovery actions.
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 5** CP-8, PE-9, PE-11, PM-8, SA-20	This helps with identifying secondary and tertiary components that are critical in supporting the organization's core business functions. This is needed to prioritize contingency plans for future events and emergency responses to ransomware events.
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 5 -** all	Establishing and communicating policies needed to prevent or mitigate ransomware events is essential and fundamental to all other prevention and mitigation activities.
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 5** - all	This is necessary for cybersecurity policy development and for establishing priorities in contingency planning for responses to future ransomware events.
	ID.GV-4: Governance and risk management processes address cybersecurity risks **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 5** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	Ransomware risks must be factored into organizational risk management governance in order to establish adequate cybersecurity policies.

Category	Subcategory and Selected Informative References	Ransomware Application
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	Identifying and documenting the vulnerabilities of the organization's assets supports developing plans for and prioritizing the mitigation or elimination of those vulnerabilities, as well as contingency planning for evaluating and responding to future ransomware events. This will reduce the likelihood of a ransomware outbreak.
	ID.RA-4: Potential business impacts and likelihoods are identified **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 5** RA-2, RA-3, SA-20, PM-9, PM-11	Understanding the business impacts of potential ransomware events is needed to support cybersecurity cost-benefit analyses as well 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.
	ID.RA-6: Risk responses are identified and prioritized **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 5** PM-4, PM-9	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 Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 5** PM-4, PM-9	Establishing and enforcing organizational policies, roles, and responsibilities is dependent on stakeholders agreeing to and managing effective risk management processes. The processes should take into consideration the risk of a ransomware event.
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 5** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9	Ransomware contingency planning should be coordinated with suppliers and third-party providers, and planning should include provisions for testing planned activities. The plan should include a scenario where suppliers and third-party providers are impacted by ransomware.

215

Category	Subcategory and Selected Informative References	Ransomware Application
Protect		
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 5** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Most ransomware attacks are conducted through network connections, and because ransomware attacks often start with credential compromise, proper credential management is an essential mitigation, although not the only mitigation needed.
	PR.AC-3: Remote access is managed **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15	Most ransomware attacks are conducted remotely. Management of privileges associated with remote access can help to maintain the integrity of systems and data files to protect against insertion of malicious code and exfiltration of data. Using multi-factor token-based authentication will reduce the impact of account compromise.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	Many ransomware intrusions occur through the compromise of user credentials or by invoking processes that should not be authorized to have privileged access to the process that is being infiltrated.
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 5** AC-4, AC-10, SC-7	Network segmentation or segregation can limit the scope of ransomware events by preventing malware from proliferating among potential target systems (e.g., moving laterally into an operational technology or control system from a business information technology network).

Category	Subcategory and Selected Informative References	Ransomware Application
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions **ISO/IEC 27001:2013,** A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	Compromised credentials are a common attack vector in ransomware events. Identities should be proofed and then bound to a credential (e.g., two-factor authentication of formally authorized individuals) to limit the infiltration potential that enables ransomware attacks.
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 5** AT-2, PM-13	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.
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-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 5** SC-16, SI-7	Integrity checking mechanisms can detect tampered software updates that can be used by criminals to insert malware that can lead to ransomware events.
	PR.DS-7: The development and testing environment(s) are separate from the production environment **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 5** CM-2	Keeping development and testing environments separate from production environments can prevent ransomware from promulgating from development and testing systems into production systems.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 5** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	Baselines are useful for establishing the set of functions a system needs to perform and that any deviation from that baseline could be evaluated for its cyber risk potential. Unauthorized changes to the configuration can be used as an indicator of a malicious attack, which may lead to the introduction of ransomware.

Category	Subcategory and Selected Informative References	Ransomware Application
	PR.IP-3: Configuration change control processes are in place **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 5** CM-3, CM-4, SA-10	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.
	PR.IP-4: Backups of information are conducted, maintained, and tested **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 5** CP-4, CP-6, CP-9	Regular backups that are maintained and tested are essential to timely and relatively painless recovery from ransomware events.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 5** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	Response and recovery plans should include ransomware events.
	PR.IP-10: Response and recovery plans are tested **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 5** CP-4, IR-3, PM-14	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.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 5** MA-4	Remote maintenance provides an access channel into networks and technology which, if not managed, criminals may use to alter configurations in a manner that permits introduction of malware.

Category	Subcategory and Selected Informative References	Ransomware Application
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 5** AU Family	Availability of audit/log records can assist in detecting unexpected behaviors and support forensics response and recovery processes.
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 5** AC-3, CM-7	Maintaining the principle of least functionality may prevent malware from proliferating laterally among potential target systems (e.g., moving into an operational process control system from an administrative network).
Detect		
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-4:** Impact of events is determined **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3, SI-4	Determining the impact of events can inform response and recovery priorities for a ransomware attack.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events **NIST SP 800-53 Rev. 5** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	Network monitoring might detect intrusions before malicious code can be inserted or large volumes of information are encrypted and exfiltrated.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	Monitoring personnel activity might detect insider threats or insecure staff practices or compromised credentials and thwart potential ransomware events.
	DE.CM-4: Malicious code is detected **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 5** SI-3, SI-8	Detection may indicate that a ransomware event is occurring. Also, malicious code is often not immediately executed, so there may be time between insertion of malicious code and its activation to detect it before the ransomware attack is executed.

Category	Subcategory and Selected Informative References	Ransomware Application
	DE.CM-5: Unauthorized mobile code is detected **ISO/IEC 27001:2013 A.12.5.1, A.12.6.2** **NIST SP 800-53 Rev. 5** SC-18, SI-4, SC-44	Detection may indicate that a ransomware event is occurring. Often malicious mobile code is not immediately executed. There may be time between insertion of malicious mobile code and its activation to detect it before the ransomware attack is executed.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 5** CA-7, PS-7, SA-4, SA-9, SI-4	Monitoring external service provider activity might detect ransomware events and other cybersecurity events before they have a chance to spread within the organization.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Monitoring can detect many ransomware attacks before they are executed.
	DE.CM-8: Vulnerability scans are performed **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 5** RA-5	Regular scans can detect most vulnerabilities before they are used to execute ransomware attacks.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14	Accountability encourages adherence to organizational policies and procedures to help detect ransomware attacks.
	DE.DP-2: Detection activities comply with all applicable requirements **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 5** AC-25, CA-2, CA-7, SR-9, SI-4, PM-14	Consistent adherence to organizational policies and procedures is necessary for detection activities to be effective against ransomware attacks.

Category	Subcategory and Selected Informative References	Ransomware Application
	DE.DP-3: Detection processes are tested **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 5** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14	Testing provides assurance of correct detection processes for ransomware-based attacks, but not that all intrusion attempts will be detected.
	DE.DP-4: Event detection information is communicated **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA-5, SI-4	Timely communication of anomalies is necessary to remediation before a ransomware attack can be launched.
	DE.DP-5: Detection processes are continuously improved **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 5,** CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	Ransomware attacks are continuously being refined, so detection processes must continuously evolve to keep up with new threats.
Respond		
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8	Immediate execution of the response plan is necessary to stop any corruption or continuing exfiltration of data, stem the spread of an infection to other systems and networks, and initiate preemptive messaging.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3, IR-8	Response to ransomware events include both technical and business responses. An efficient response requires all parties to understand their roles and responsibilities.
	RS.CO-2: Incidents are reported consistent with established criteria **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8	Response to ransomware events include both technical and business responses. An efficient response requires pre-established criteria for reporting and adherence to that criteria during an event.

Category	Subcategory and Selected Informative References	Ransomware Application
	RS.CO-3: Information is shared consistent with response plans **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 5** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	Information sharing priorities include stemming the spread of an infection to other systems and networks as well as preemptive messaging.
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	Coordination priorities include stemming the spread of misinformation as well as preemptive messaging.
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 5** SI-5, PM-15	Information sharing may also yield forensic benefits and reduce the impact and profitability of ransomware attacks.
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	Sometimes what is detected is the testing of a ransomware attack that can be preempted.
	RS.AN-2: The impact of the incident is understood **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 5** CP-2, IR-4	Understanding the impact will shape the implementation of the recovery plan.
	RS.AN-3: Forensics are performed **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 5** AU-7, IR-4	Forensics help identify the root cause to eradicate the ransomware and can inform the recovery process.

Category	Subcategory and Selected Informative References	Ransomware Application
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) **NIST SP 800-53 Rev. 5** SI-5, PM-15	This can prevent future successful attacks and the spread of the ransomware to other systems and networks. It can also help restore confidence among stakeholders.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 5** IR-4	Immediate action must be taken to prevent the spread of the ransomware to other systems and networks.
	RS.MI-2: Incidents are mitigated **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 5** IR-4	Immediate action must be taken to isolate the ransomware to minimize the damage to the data, to prevent the spread of infection to other systems and networks, and to minimize the impact on the mission or business.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks **ISO/IEC 27001:2013 A.12.6.1** **NIST SP 800-53 Rev. 5** IR-4	This is necessary to minimize the probability of future successful ransomware attacks or understand the risk and to restore confidence among stakeholders.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned **ISO/IEC 27001:2013 A.16.1.6,** Clause 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	This is necessary to minimize the probability of future successful ransomware attacks and to restore confidence among stakeholders.
	RS.IM-2: Response strategies are updated **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev 5** CP-2, IR-4, IR-8	This is necessary to minimize the probability of future successful ransomware attacks and to restore confidence among stakeholders.

Category	Subcategory and Selected Informative References	Ransomware Application
Recover		
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8	Immediate initiation of the recovery plan after the root cause has been identified can cut losses.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev 5** CP-2, IR-4, IR-8	This is necessary to minimize the probability of future successful ransomware attacks and to restore confidence among stakeholders.
	RC.IM-2: Recovery strategies are updated **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8	This is needed to maintain the effectiveness of contingency planning for future ransomware attacks.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4	This is necessary to minimize the business impact by being open and transparent and to restore confidence among stakeholders.
	RC.CO-2: Reputation is repaired after an incident **ISO/IEC 27001:2013** Clause 7.4	Repair is necessary to minimize the business impact and restore confidence among stakeholders.
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 5** CP-2, IR-4	Communication of recovery activity helps to minimize the business impact and restore confidence among stakeholders.

References

[1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (2013) Information technology—Security techniques—Information security management systems—Requirements. (International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland), ISO/IEC 27001:2013. https://www.iso.org/isoiec-27001-information-security.html

[3] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5