CYBERSECURITY
COLLABORATIVE

A CyberRisk Alliance Community

Addressing the Ransomware Threat

Best Practices Guidance Document

A Cybersecurity Collaborative Task Force Product

Table of Contents

"Razing" Ransomware Task Force Members and Acknowledgements

The Cybersecurity Collaborative would like to acknowledge the following member companies and individuals for their collaborative efforts which, through discussions, experience, and research, provided the content for this document.
Please direct any questions to members@cyberleadersunite.com

TASK FORCE EXECUTIVE LEADERS:

SHELDON CUFFIE
CISO, American Family Insurance

ARLAN MCMILLAN
CSO, Kirkland and Ellis

TASK FORCE MEMBERS (CISOS AND SECURITY STAFF):

BENJAMIN CORLL
CISO, Coats

SHOLLOM ELLENBERG
CISO, JASA

JOHN GERMAIN
CISO, Duck Creek Technologies

BRYAN HURD
CISO, Aon

RICHARD RUSHING
CISO, Motorola Mobility

MATT STIAK
CISO, Delta Dental

BRIAN WEIDNER
CISO, Nissan

STEVE YURICH
CISO, Penn National Insurance

JILL BURDICK-ZUPANCIC
Lead Associate, Booz Allen Hamilton

DOUG DEMIO
AVP of Cyber/RTF, American Family Insurance

MATTHEW DUNLOP
Cybersecurity Analyst, JASA

VIPIN GOPAL
Senior Security Architect, Duck Creek Technologies

MITCH GREENFIELD
Director, Core Architecture | Enterprise Information Protection (EIP), Humana

TALMADGE HEWITT
Director, Contingency Planning, Union Pacific

JONI MCLEAN
Crisis Management Senior Consultant, Nationwide

JOHN NAGENGAST
Sr. Information Security Architect, Penn National Insurance

JOSH SLADE
Lead Endpoint Security Architect, Humana

KRISTY WESTPHAL
Director, Information Security and Operations, Healthequity

Introduction

Background and Purpose

In August 2021, members of the Cybersecurity Collaborative organized a task force to develop best practices for addressing the ransomware threat. Experience from ransomware attacks and the threat's prevalence, impact, and growth motivated members to collaborate on identifying the most effective strategies for preventing, detecting, and responding to a ransomware attack.

Member discussions, experiences, and contributions, including policies, decision criteria (e.g., whether to pay a ransom), and presentations to senior management, contributed to developing best practices presented in this document. CISOs can use this document to help develop effective prevention, detection, and response strategies or refocus their efforts on more cost-effective plans.

The organization of this guidance document is as follows:

- "The Evolving Ransomware Threat" presents growth, tactics, and impact statistics on the ransomware threat.

- "Preparation Steps to Strengthen Ransomware Defense & Response Capabilities" provides guidance for CISOs looking to organize and prepare for the threat.

- "Assessing Current Ransomware Preparedness Capabilities" presents the Cybersecurity Collaborative Ransomware Preparation Assessment (CSC-RPA)).

- "The Strategy & Implementation Plan Development" helps CISOs evaluate and prioritize strategic options for inclusion in an implementation plan.

- "Additional Member Guidance" gives member guidance on different topics, including incident management and pay-no-pay decisions.

- "Appendix: Ransomware Security Controls" provides the following information for each of the twenty-one controls: description, relative costs, implementation difficulty, value, and member guidance on implementation and use. This document is for the benefit of members of the Cybersecurity Collaborative. It may not be distributed to non-member organizations or individuals without the consent of authorized Cybersecurity Collaborative management. References to company names or products are examples and are not endorsements by the Cybersecurity Collaborative.

Characteristics of the Ransomware Threat that Guided the Development of this Document

Although the prospect of a ransomware breach is frightening, the threat characteristics do not alter the security fundamentals that enterprises and government agencies currently embrace. Maintaining and improving a comprehensive security program modeled on an industry standard, like NIST or ISO, is the best overall defense against ransomware.

However, characteristics of the ransomware threat have required entities to focus on a subset of controls. For example, by encrypting data, ransomware mimics the effect of a denial-of-service attack. Therefore, to avoid paying for a decryption key, entities must deploy effective backup, recovery, incident management, and business continuity processes. Additionally, by exfiltrating data, ransomware agents can threaten to expose data if the entity does not pay the ransom. Therefore, companies must implement controls, like encryption, to prevent data from being maliciously used by a ransomware agent.

Businesses and governments do not want to be victims of a ransomware attack. Therefore, they must focus on controls that detect and contain an attack, like extended detection and response (EDR) technologies, and controls that stop the spread of an attack, like strong-privileged access and configuration management.

Based on these characteristics, the Ransomware Task Force identified twenty-one security controls that specifically target the ransomware threat. Task force members then categorized them according to the NIST Cybersecurity Framework and further described them in the Appendix.

Supplemental Tools

The Cybersecurity Collaborative task force members created the following supplemental tools to support the guidance provided in this document. These are available to members under separate covers:

1. CSC Ransomware Preparedness Assessment (CSC-RPA). The CSC-RPA evaluates twenty-one controls that are key to addressing the ransomware threat. The CSC-RPA generates an assessment score and heatmap to help develop strategies and plans.

2. Incident Response Reference Architecture. This tool aligns with the MITRE framework and shows where and how technologies can support incident response processes.

3. Boardroom Education Materials. These materials include a primer on board member security responsibilities and education about ransomware characteristics and risks.

4. Pay-No-Pay Decision Criteria. These decision criteria include legal and ethical considerations to help executives make an informed decision about paying ransoms.

The Evolving Ransomware Threat

At task force meetings, members reviewed CSC Morning Security Report articles and other reports to arrive at the following conclusions regarding the nature and growth of the ransomware threat.

Ransomware Pervasiveness and Growth

Ransomware is highly pervasive with projected exponential growth rates.

According to Positive Technologies, ransomware comprised 69% of all malware attacks during the second quarter of 2021. Compared to last year, this represented a 30% increase over the same period. Attackers preferentially targeted government, industrial, medical, education, and scientific organizations.

A SonicWall ransomware growth chart shows that the number of ransomware attacks almost doubled between Q1 2020 and Q1 2021, from 60 million to 116 million. The 2021 Verizon Data Breach Investigations Report shows ransomware as one of the four top actions taken in breaches.

Ransomware breaches almost occur daily.

As shown in Figure 1, companies in various business sectors, including healthcare, banks, media, communications, and agriculture, are reporting attacks.

Figure 1. Companies Breached by Ransomware (8/31-10/19/21)
(Source: CSC Morning Security Report)

Threat Actor Tactics, Techniques, and Procedures

The number of threat vectors is increasing.

A threat vector is a method by which a ransomware agent gains a foothold into an entity's computing environment. When the threat agent uses their point of entry to exploit network vulnerabilities, they spread malware and increase the magnitude of adverse impacts. In the past, the most common threat vectors were phishing emails, remote desktop protocol (RDP) vulnerabilities, and website vulnerabilities.

An analysis of ransomware breaches reported in the CSC Morning Security Report shows that ransomware agents are successfully gaining footholds using other threat vectors. The most popular are unpatched vulnerabilities on older systems, brute force password attacks, SQL injection flaws, and attacks on backup systems.

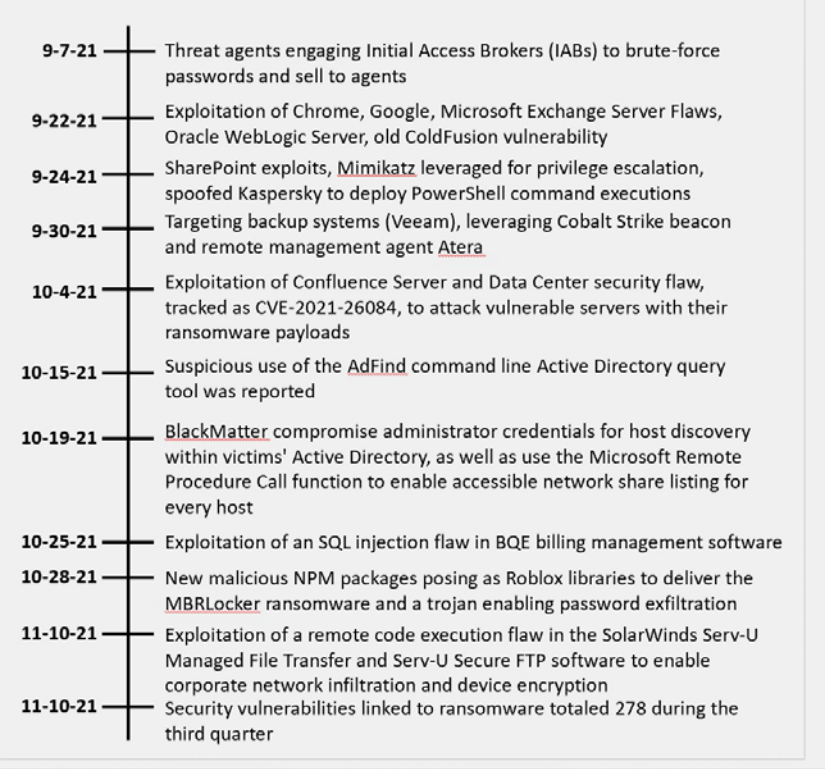

Figure 2. Threat Vectors Used for Successful Ransomware Attacks (9/17-11/10/21)
(Source: CSC Morning Security Report)

Ransomware agents are finding more ways to extort victims.

Ransomware agents typically extorted victims by demanding payment for a decryption key. However, agents now threaten to release stolen confidential information if the victim does not pay the ransom, known as a "double extortion." If the victim still resists paying the ransom, ransomware agents will threaten to contact the victim's customers or attack their systems based on the confidential information gained, known as a "triple extortion." They also frequently warn their victims not to engage law enforcement or a negotiator.

Impacts and Payouts

Damage costs, in the form of payouts or restoral costs, are currently in the billions of dollars and are expected to increase tenfold this decade.

According to a Sophos report, the average ransomware payout doubled between Q1 2020 and Q1 2021 from $20,000 to $54,000, with education, distribution and transport, business and professional service, retail, IT technology and telecommunications, and financial service sectors are experiencing above-average costs and payouts. Chainalysis reports the highest known payment at $10 million.

Company and Government Responses

Companies believe they are unprepared for ransomware attacks.

According to Dell's 2021 Global Protection Index, sixty-seven percent of IT decision makers expressed concern regarding their inability to recover data compromised by ransomware and other cyberattacks. Eighty-two percent believe that current data protection measures will no longer suit their businesses' future needs. Sixty-two percent state that existing data protection measures are inadequate against ransomware and malware threats.

Governments are taking more initiative to address the threat.

Recognizing the seriousness of the threat, the US is cooperating with foreign governments to share information and sanction cryptocurrency exchanges that allow ransomware payments.

Law enforcement is actively targeting ransomware groups. In October 2021, the US partnered with other countries to hack and disrupt the Russian-led REvil ransomware gang, which had impacted Colonial Pipeline.

Steps to Strengthen Ransomware Defense & Response Capabilities

Introduction

The prevalence of ransomware and its potential consequences require CISOs to take decisive actions to improve their security programs. These actions begin with the implementation of the following four steps.

Step 1: Communicate Concerns and Intentions with Executives

As shown in Figure 1, companies in various business sectors, including healthcare, banks, media, communications, and agriculture, are reporting attacks.

As a CISO, it is good to be genuinely concerned about the possibility of a ransomware attack. Executives and board members are also likely to be worried. However, whether they state so explicitly or implicitly, they need a CISO's guidance and leadership to develop and execute plans that address those concerns.

At an executive committee meeting, approach the CEO and key subordinates with concerns and a plan to strengthen your organization's ransomware defenses and response capabilities. Ask for 15 to 20 minutes on the agenda and present a short deck of fewer than ten slides for discussion. Slide content should include:

1. Industry statistics about ransomware tactics, growth, and impact.
2. Information about the scope of ransomware targets and critical stakeholders within that environment.
3. The need to assess current defenses and response capabilities to develop improvement plans.
4. The importance of establishing a ransomware task force to expedite assessment, planning, and execution.

After the discussion, gain permission to engage in activities that meet the above requirements. Plan a date for the executive committee to review the company's progress and then set up regular review dates.

Step 2: Scope the Environment

CISOs leading an organization's ransomware defense and response capability improvement efforts may not have direct control over all the technology environments in the company. For example, the operations technology team, which operates manufacturing systems, may have its own CIO and security group. Large, multinational organizations may have multiple CIOs and CISOs.

While it can be tempting to develop plans only for specific scopes, doing so may undermine the strength of defensive and response controls. Ransomware can attack any technology environment connected directly to the internet and then move laterally to internal networks. Therefore, improvement plans need to define scope by potential ransomware targets and spread, not by organizational responsibilities. This collaboration requires coordinating with peers in other organizations.

Step 3: Identify Key Stakeholders

Stakeholders are organizations and individuals responsible for implementing and operating security controls that identify, protect, detect, respond to, and recover from a ransomware attack. The environmental scoping exercise will identify most stakeholders, which fall into the categories shown in Table 1:

Category	Responsibilities	Individuals/Organizations
Executive Management	• Informed by CISO or an Incident Response Team of a ransomware event, its impact, and containment efforts • Provides communications to board, customers, press, law enforcement • Decides or endorses the decision to pay a ransom	CEO, CFO, Legal, Corporate Communications, Chief Privacy Officer, Chief Ethics Officer
Technical Management	• Manages ransomware incident • Reports incident status to executive management	CIO or CTO, Chief Security Officer, Chief Operations Officer
Technical Support Organizations	• Supports incident management capabilities • Implements and operates protection controls	Security Operations (SOC), Security Engineering, IT Operations, IT Applications
Outside Support	Provides several types of support, including: • Negotiation • Identifying and prosecuting perpetrators • Insurance to cover losses • Business Continuity Plan and Disaster Recovery (BCP/DR) support • Identification of ransomware characteristics	Ransomware Negotiator, Law Enforcement, Cyber Insurance agency, Disaster Recovery sites, Forensics Organizations

Table 1. Key Stakeholder Categories, Responsibilities, and Individuals/Organizations

Step 4: Establish a Ransomware Task Force

After identifying key stakeholders, organize a task force dedicated to improving the organization's ransomware defense and response capabilities. Cybersecurity Collaborative Members have found that a dedicated ransomware task force enables the organization to rapidly implement many improvements, like shortening containment and recovery timeframes. Consider forming a team that includes minimally the following expertise: BCP/DR, security engineers, communications, risk analysis, and program management to coordinate with different delivery teams.

Assessing Current Ransomware Preparedness Capabilities

Introduction

After completing the steps above, it is necessary to assess the entity's current capabilities to detect, protect, and respond to a ransomware threat. The assessment's outcome will drive the development and prioritization of various capability improvement strategies.

Different assessment options are available, such as engaging a consulting firm with expertise in ransomware. While this option promotes objectivity, it may also be more costly than a self-assessment. Several member-cited organizations offer free self-assessments, such as the Conference of State Bank Supervisors, the Secret Service, and the Cybersecurity and Infrastructure Security Agency. Security systems providers may also provide assessment tools, although sales may be the desired outcome of using the service.

Inspired by a task force member, the Cybersecurity Collaborative has developed a preparedness questionnaire for its members, as described below.

CSC-RPA: The Cybersecurity Collaborative Ransomware Preparedness Assessment

The CSC-RPA assesses the strength of twenty-one key controls that members considered relevant to preventing, detecting, and responding to ransomware. After reviewing each control, task force members documented control components, value for addressing the ransomware threat, implementation difficulty, and relative cost. Following this analysis, they created a questionnaire that generates a preparedness score, control heatmap, and recommended strategies for improving control strength.

Below are descriptions and screenshots from the questionnaire, preparedness score, and control heatmap.

Questionnaire

The questionnaire consists of twenty-four questions, organized as dropdown choices and checkboxes. Figure 3 represents a screenshot of the questionnaire.

Protected Backups	Which statement most closely describes the extent to which key data, systems, and configurations are independently backed up (full and incremental backups)?	Separate full and incremental backups of key data, systems, and configurations ARE NOT taken.	
Clean Environment Recovery	Which statement most closely describes the extent to which key data, systems, and configurations are restored to an environment that has been "cleaned" of ransomware?	Applications, systems and configurations ARE NOT restored in an environment not impacted by ransomware	

		ASSETS	PERCENT OF ASSET POPULATION					COMMENTS
			< 25%	26-50%	51-75%	76-90%	>90%	
Local Admin Contrl	Local administrative rights is restricted/controlled for what percent of relevant assets?	Laptops/workstations	☑	☐	☐	☐	☐	
			< 25%	26-50%	51-75%	76-90%	>90%	
Awareness (Phishing Exercises)	Phishing exercises are conducted for what percent of the user population?	Employees and relevant contractors	☐	☐	☐	☐	☑	

Figure 3. Screenshot of the CSC-RPA Questionnaire

Preparedness Score

Responses to the questionnaire generate a preparedness score, as shown in Figure 4, below. Each questionnaire response has a numerical value assigned to it. This value reflects the extent control components are implemented over the percent of applicable assets. For example, the value for local administrator controls reflects the number of requirements implemented, such as removing local admin from desktops and providing a means for users to install requested applications, and the percent of desktops currently covered by the control. If the organization takes the assessment at different time intervals, the Preparedness Score will reflect those improvements.

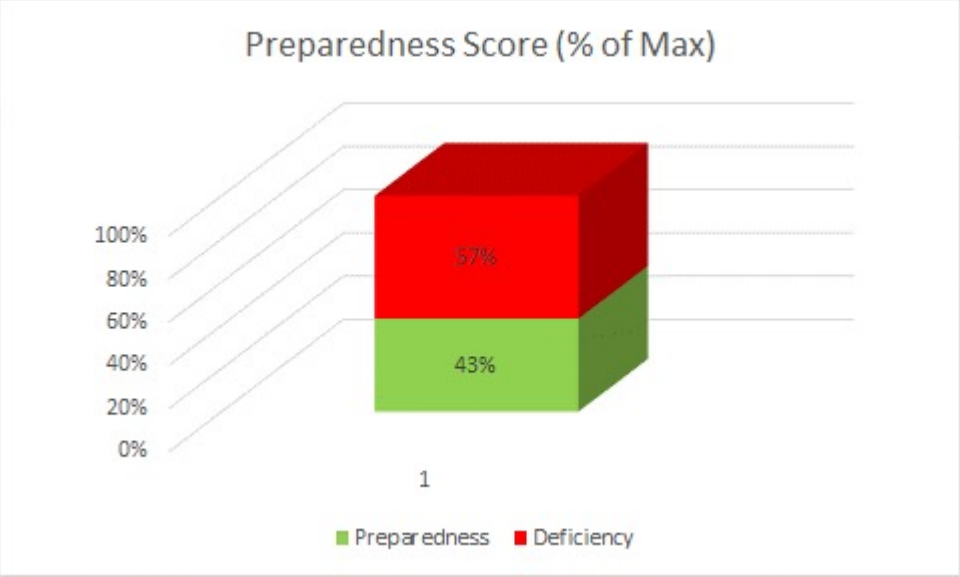

Figure 4. Example CSC-RPA Preparedness Score

Control Heatmap

Responses to the questionnaire also generate a Control Heatmap, as shown in Figure 5. CISOs can use this heatmap to represent the current effectiveness of their ransomware controls to management. Retaking the assessment after making control improvements will change the heatmap, potentially demonstrating progress.

Figure 5. Sample CSC-RPA Control Heatmap

Strategy & Implementation Plan Development

Evaluate Strategic Options

The CSC-RPA also generates a list of improvement strategies, rated as red or yellow on the heatmap in Figure 6, below. CISOs should start by considering the improvement strategies for critical controls rated red, followed by those with yellow ratings.

Control	Components	Value	Implementation Difficulty	Relative Cost	Rating	Improvement Strategy
Exec. Awareness, Concern, Support	1. Aware of threat 2. Concerned about threat 3. Support with resources	Critical	Low	Low		Reach out proactively to executives with impact of threat and results of Assessment
Resources (Budget & Staffing)	1. Financial resources to address ransomware control deficiencies 2. Sufficient staff resources to respond to and recover from a ransomware attack.	Critical	Medium	Low		Following development of strategies prepare a budget of incremental costs (technology implementations, staff support)

Figure 6. CSC-RPA Control Improvement Strategies

To prioritize improvement strategies for non-critical controls, CISOs can reference Figure 7, which shows cost, effectiveness, and implementation tradeoffs.

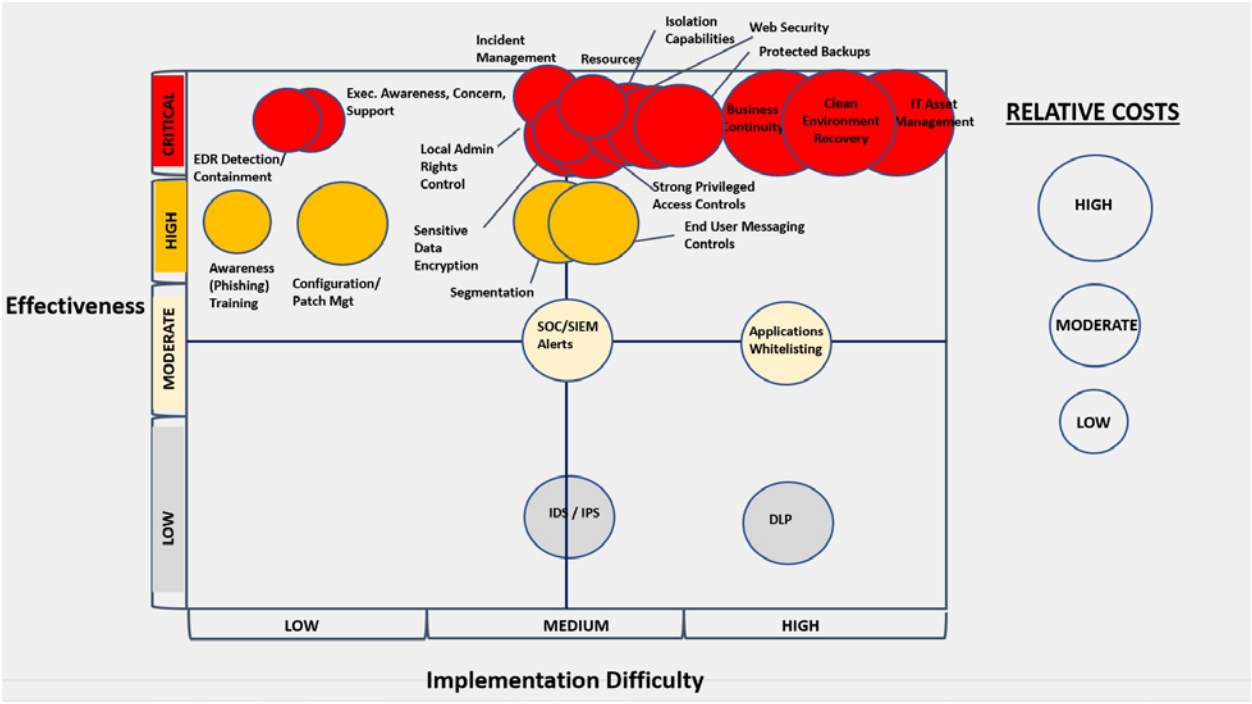

Figure 7. CSC-RPA Control Cost, Effectiveness, Implementation Matrix

CISOs managing an organization with immature ransomware controls may opt to engage in a "Quick" Strategy, described in Figure 8. The Quick Strategy is designed to focus on a subset of key controls that will provide the greatest protection in the shortest period of implementation time.

OBJECTIVE	CONTROLS	GUIDANCE
1. Be able to recover operationally	• Protected Backups • Clean Environment Recovery • Business Continuity / DR	• Failover is not an effective backup strategy • Restore to a clean environment • Must restore system configurations
2. Be able to detect and respond quickly and decisively	• EDR Detection & Response Capabilities • Isolation Capabilities • Incident Management	• Detect ransomware events as well as failed login attempts • Permission and capability to isolate/shut down systems & networks • Establish and test pay/no pay decision criteria
3. Implement the most effective protection measures	• Local Admin. Rights Controls • Sensitive Data Encryption • Strong Privileged Access Controls • Awareness (Phishing) Training	• Phishing training as high value, low cost • Removing local admin rights on laptops helps prevent malware installs

Figure 8. "Quick" Strategy

Develop and Communicate an Implementation Plan

CISOs should develop action plans for selected strategies and estimate their costs before reviewing plans and costs with executive management. Following approval, use the entity's project management organization and tools to develop a detailed implementation plan with budgets, assignments, timeframes, and milestones.

Additional Member Guidance

This section lists member guidance associated with key security topics or controls.

Board and Management Communications

- **How is the discussion of ransomware framed for the board?**
    - Ransomware is not a topic unto itself: it is discussed as one threat among many
    - Need to socialize ransomware threat.
    - The Finance Committee needs to know the potential impact of a ransomware incident:
        - Estimate the impact in dollars by multiplying the number of company records by the cost per record breached.
        - Consider how much both ransom and restoral are likely to cost.
        - Discuss what a cyber insurance policy will cover and not cover.
    - May also need to discuss cybersecurity with the Audit Committee.

- **What content is often shown to the board?**
    - At the annual State of the Union, discuss the major elements of the threat landscape, such as double or triple extortion.
    - Throughout the year, bring up specific incidents and news-worthy stories, like SolarWinds, and discuss the outcomes.
    - Always put ransomware in the context of enterprise risk capabilities.

- **Walkthrough of a boardroom presentation:**
    - Show critical incidents over the last six months, using aliases to avoid e-discovery.
    - List of attacks and status, per the NIST model.
    - Internal audit findings, if the company has a partnership with an auditor.
    - Note any brand damage, supplier disruption, sales disruption, or business disruption that has occurred.
    - Show a risk matrix for ransomware:
        - X-axis: Impact: low, high
        - Y-axis: Likelihood: low, high
        - Put all suppliers, third parties, and enterprise customers with the matrix
    - Control maturity measures may be used to show improvements to the security program over time, if they are socialized with management and not perceived as subjective measures.

Additional Member Guidance (cont.)

Business Continuity Management and Disaster Recovery

- **Ransomware's Shift to BCM/DR Approaches:**
    - The business continuity paradigm is very different when a company is recovering from a natural disaster to recovering data and its integrity after a ransomware attack.
    - There is a difference between restoring one and two systems and most of your systems. Your recovery time objectives are going to be different. Many organizations have not thought about what systems to bring up first if they have lost most or all of their systems.
    - Recognize that in addition to restoring applications, you will be restoring AD, DNS, network, and core infrastructure systems. Companies need to get a database up and running before restarting applications.
    - Recovering systems in the wrong order can corrupt databases, so think through the order of operation and dependencies.
    - Make sure you are backing up code in DevOps.
    - If you lose the domain controller, you will need to rebuild it.
    - Restoral processes are situational. There is a difference between a large outage and a single outage.
- **Backup:**
    - Raise awareness of how to recover from backups, including decentralized backup restoration, using offsite facilities like cloud offerings.
    - Use WORM (Write Once, Read Many) technology so users cannot write over backups.
    - Airgap operating environments to limit lateral transmission, thereby corrupting backups.
    - Backup processes should occur over 30, 60, and 90 days.
- **Restoral:**
    - Ensure that the restoral environment is clean of ransomware to prevent integrity violations.
    - Restore onto a separate network.
    - Need to know the software version you are restoring.
    - Employ deep scanning technologies.

Incident Management

- **Documentation:**
    - Create an incident response playbook specifically for ransomware, including:
        - Updated information retrieval architecture and response, such as blending MITRE ATT&CK with threat intelligence and overlay automation.
        - Pay or not pay decision criteria.
    - Always include a crisis communications plan.

Additional Member Guidance (cont.)

- **Organizations and Their Roles:**
    - SOC/Operations Teams/Cyber Fusion Center
        - Strengthen their capability to identify and take unilateral actions, such as network blocks, shutdowns, and device isolation, to contain ransomware.
        - Ensure management signs off on the corporate policy allowing operations teams to take unilateral action.
        - Set up a war room, either physical or virtual.
    - Know who is on the cyber incident response team (CIRT). Consider including legal, communications, and marketing experts and potentially a breach coach.
    - Assign one person to deal with Help Desk and third parties inquiries
    - Ensure any public relations or corporate communications team knows what to write in terms of the company's public response to a breach.
    - Establish a dedicated ransomware response team as a second-tier defense.
    - For specific member organizations, the CISO was the incident commander for any ransomware incident.
- **External Resources Used:**
    - Breach coach:
        - Cyber insurance agencies will recommend breach coaches, like Ironshore and Coveware.
        - Once on retainer, they can set up a Bitcoin account to use in negotiations
        - They can buy time, negotiate a lower payout, and determine if data has leaked.
    - A forensics team on retainer, such as SecureWorks, can help conduct tabletop exercises.
    - External media relations firm.
- **Incident Severity Rating:**
    - High-severity incidents involve the extended CIRT.
    - Members automatically categorized ransomware as a high-severity incident.
- **Testing:**
    - Tabletop tests should be performed after defining roles and responsibilities, so participants gain experience in their specific role. They also demonstrate the chaos of an event.
    - Document and address deficiencies that arise from the test.
    - Involving senior management in tests may support your case for added resources when deficiencies present themselves.
    - Task force members have used both internal and external resources to conduct tests. Internally led tests can identify deficiencies, while externally led tests can engage executives and educate them on the likelihood of finding weaknesses.
    - Combine communications with the executive level. Involve CPO, CISO, legal department, corporate communications, technology teams, call centers, sales, and marketing teams.

Pay-No-Pay Ransom Decision Criteria

- **General Guidance:**
    - Work within a framework, such as policies and flowchart decision criteria.
    - Test different scenarios within the framework.
    - Go through the decision process in advance of the ransomware attack.
    - Decide who should offer advice and who makes the final decision.
    - Be sure to meet any cyber insurance requirements and regulations.
    - Decide who makes recommendations, who approves, and who owns the decision.
    - Perceive ransomware broadly as a means of extortion, like kidnapping and ransom. As such, extend possible breaches to include ransoming executives by breaching home systems.
    - Remember that ransomware agents use payments to fund future crimes, including cybercrime.
    - Social and ethical responsibilities must be considered when deciding to pay; involve your Chief Ethics Officer in those decisions.
    - Think carefully about the systems you are protecting from ransomware, in terms of the impact of not having those systems operational (e.g., shutting down production).
- **Groups Involved in Decision Making:**
    - Even if there is a group discussion, one person needs to own the decision.
    - InfoSec can make the decision, but the CEO can overrule it.
    - Members have not seen decision making elevated to the board.
    - Decision-making should include the privacy team, government relations, general legal counsel, CIO, CISO, business units, finance, and human resources.
    - Outside groups supporting the decision-making process can include outside counsel, insurance, ransomware negotiator, and law enforcement.
- **Member-Contributed Decision Criteria**
    - **Moral and Ethical:** Weigh funding criminal or terrorist activity against the impact on customers and partners.
    - **Business and Technology Continuity:** How much of our data can we recover and how quickly? Consider critical operations independently from full recovery.
    - **Operational Impact:** Is this an existential threat? What are the direct and indirect financial impacts from loss of operational capability?
    - **Regulatory, Compliance, and Reporting:** Regardless of payment, there are federal, state, and group reporting obligations, each of which has a set deadline to report the incident. Are there specific obligations to report a ransomware payment? When should law enforcement be contacted? Which agencies?
    - **Reputation and PR:** Consider providing transparency into this decision-making process. What mandatory reporting will become public knowledge?
    - **Legal:** Making a ransom payment may jeopardize a non-profit status. Criminal and civil penalties exist for transacting with individuals or entities sanctioned by OFAC. Other government bodies may impose additional sanctions after ransom payments.

Additional Member Guidance (cont.)

- **General Guidance:**
    - **Law Enforcement:** Engaging law enforcement may be a prerequisite for recovering ransom funds via criminal seizure. However, law enforcement may take control of the investigation, limiting options to respond, recover, or pay.
    - **Threat Actor:** We cannot trust that a threat actor will act honorably; however, neither should a double-cross be presumed. Public knowledge that a company paid a ransom may increase the likelihood of being targeted in future attacks.
    - **Recovery of Funds:** It may be possible to recover some or all the ransom through civil or criminal asset seizure or by filing an insurance claim.
    - **Liability:** If the threat actor publishes our data or uses it to extort members, employees, groups, partners, etc., what liability does the company have?
    - **Cyber Insurance:** Our carriers may impose constraints on claims filed for ransom payments. Those include the deductible, ransom-specific limits, or requirements to engage specific third-party incident response firms or ransomware experts.
    - **Logistical:** How will we obtain the currency in which the ransom is demanded, such as Bitcoin? Are there fees or overhead associated with obtaining this currency? What will we have to pay our negotiator?

Other Areas

- **Working at Home**
    - Focus on remote connections without external RDP.
    - Ensure that all connections are web-based.
    - Deploy Chromebooks, so there is no local data storage.
- **Third-Party Risks**
    - Ensure suppliers do not have direct access to company networks.
    - Use a VPN connection and allow API access
    - Use of endpoint detection and response (EDR) technology helps reduce the risks of a successful ransomware attack
    - Know who has access to what when coming in through virtual desktop infrastructure

Conclusion

Conclusion

Realizing large profits from extortions, ransomware agents succeed in breaching more companies each year. As companies improve their defenses against frequently exploited threat vectors, like phishing emails, ransomware agents exploit other vulnerabilities, like unpatched systems.

Defending against ransomware attacks does not require revamping entire cybersecurity programs. However, it does require ensuring that critical defensive and response controls, like protected backups and recovery, operate consistently and effectively. It also requires CISOs to act decisively in organizing and strengthening their entities' defenses.

This guidance document will help CISOs strengthen their defense against and respond to a ransomware attack. Collaboration with Cybersecurity Collaborative peers will also help CISOs learn from other member successes and missteps.

Appendix: Ransomware Security Controls

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
Identify	Executive Awareness, Concern, Support	1. Executives are aware of the potential impact of the threat. 2. Executives accept that the threat is real and must be addressed. 3. Executives support initiatives to address the threat both financially and when making decisions.	When executives understand the threat and its impact, they will support cooperation among business units and provide additional funding	Critical	Low	Low	1. Present threat likelihood and potential organizational impacts to senior executives at standing meetings, like the executive committee and IT or privacy steering committees. a. Show names of companies impacted and their consequences, like payouts and disruptions. b. Show how a ransomware incident could specifically impact the organization. c. Identify control weaknesses and present a plan to correct them. 2. Recommend a standing meeting with executives on this topic, as regular updates are required for communication and executive guidance.
	IT Assessment Knowledge and Management	1. Inventory of all computer assets, including the sensitivity of assets. 2. Application of all security controls to inventory components,	IT Asset Management (ITAM) ensures that technical controls, such as patching and anti-malware, are operating to help prevent	Critical	High	High	1. Without an ITAM Program, companies lack compliance assurance. 2. Without an accurate inventory, entities cannot confidently say they can protect assets from a ransomware attack. 3. Axonius and Armis are next-generation ITAM technologies.
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
Identify, cont.		including anti-malware, access rights, configuration management, patching, and network access.	ransomware from executing unauthorized access.				4. If an ITAM program is not yet in place, at least provide an inventory of grouped assets by asset owners and work with owners to implement and manage necessary control. These owners should be a part of the ransomware CIRT.
	Resources (Budget & Staffing)	1. Financial resources to address ransomware control deficiencies. 2. Sufficient staff resources to respond to and recover from a ransomware attack.	Assessment of the ransomware threat may indicate significant control deficiencies, such as difficulty in recovering systems. Additional staff support from third parties and an increased budget may be required.	Critical	Medium	Low	Additional funding may be specifically required to address the ransomware threat, especially in the following areas: 1. Backups. 2. Recovery processes and testing. 3. Third-party support, such as hiring a ransomware negotiator.
Protect	Sensitive Data Encryption	1. Encryption of sensitive data stored on computing devices. 2. Protection levels and key strengths	A ransomware attacker may have administrative access to a device containing sensitive data. However, if the data are copied	Critical	Medium	Moderate	1. Need to address potential systems performance issues that stem from using encryption technologies. 2. There may be barriers to applying encryption globally, especially regarding closing USB ports.

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
		can vary. Types include: a. Device storage. b. Files. c. Column-level encryption, where cache clearing and USB encryption or lockdown are sub-controls.	and transported, the data will not be in viewable form.				
	Local Admin Rights Control	1. Remove local administrative rights on all user workstations. 2. Allow for and document business-justified exceptions. 3. Implement a process for installing approved software on user workstations.	Removing or restricting user local administrative rights on workstations prevents executing malicious software, including ransomware.	Critical	Medium	Low	1. Prevents malware from running, although some memory-resident malware can run. 2. Microsoft Local Administrator Password Solution (LAPS) is easy to implement. It removes local admin rights yet can give people temporary access. Additionally, it is audited. 3. BeyondTrust can also install programs with a shell rule.
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
Protect, cont.	Awareness (Phishing) Training	1. Implement a tool that will help users understand the characteristics of phishing emails. 2. Send phony phishing emails to users to measure compliance via clicks.	Phishing has been a primary attack vector for ransomware.	High	Low	Low	1. Consider using prevalent marketplace tools, such as Knowbe4 and PhishMe. 2. Worth the effort. Many of these tools come in 13 languages. 3. There is a landscape of different users: some have more computer experience than others. 4. Can have a negative effect where users become concerned with most emails. 5. Consistency is essential. Begin with training, then continue with phishing exercises.
	Strong Privileged Access Controls	1. Key components include: a. Basic cache clearing of credentials. b. Multi-factor authentication. c. Use and proper architecture of jump boxes.	Violating privileged access is a fundamental attack vector for gaining access to data for encryption and transport purposes.	Critical	Medium	Moderate	1. Privileged accounts must be designated and managed. 2. Consider "just in time" provisioning, where privilege is temporarily given out with a set expiration. 3. Monitoring for invalid privileged access attempts may indicate the presence of ransomware. 4. Locking down service accounts present a challenge, as application owners do not know where they are and what will break. Members are examining better ways to control these accounts, such as implementing a privileged

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
		2. Accounts are monitored for invalid logins.					access management solution, disabling interactive logins, and putting controls on to monitor them.
	Network or Systems Segmentation Network or Systems Segmentation, cont.	1. Segmenting networks devices and servers via firewalls, routers, and virtual LANs.	Segmentation may prevent or slow the spread of ransomware, improving containment efforts by giving response teams more time to react.	High	Medium	Moderate	1. Good practice, but difficult to implement as not everything can be segmented and function. 2. Can segment critical data following a least privilege model. 3. Wall off risky elements from the network. 4. During recovery, there is a contamination concern. People should not be able to take laptops and traverse networks. Controls should manage moving from unmanaged to managed networks. 5. Valuable for response efforts, as ransomware spreads quickly. Isolated networks can be shut down and dealt with later. 6. Best practice is using an EDR tool to isolate the host level rather than the net level. When a host is legitimately offline, one can be more proactive. 7. IoT devices should be isolated as much as possible, including industrial control and
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
Protect, cont.							supervisory control and data acquisition systems. 8. The original design is not often maintained, and everything gets connected. 9. The CISCO Secure Workload is a valuable segmentation tool, but it takes time to implement. 10. This control depends on the other controls, such as filtering and access controls. 11. Wireless network is controller based. The only way to shut it down is shutting down the controller, which may take down the whole organization.
	Configuration Management and Patching	1. Tools and processes to securely configure computing devices, such as servers and laptops. 2. Secure configurations include: a. A standard device configuration,	Secure configurations help prevent attackers from gaining administrative access to a device or exploiting unaddressed vulnerabilities, like an unpatched	High	Low	Moderate	1. Use a configuration management database to keep track of inventory and manage configurations. 2. Observe that ransomware is now targeting vulnerabilities.

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
		changing defaults and removing unnecessary services. b. Enable security services, such as antivirus and patching. c. Monitor the security, capacity, and availability of devices.	operating system or middleware.				
	Application Whitelisting	1. Maintain a register of approved applications. 2. Ensure that only approved applications are installed on computing devices.	Helps prevent a user or organization from installing malware.	Moderate	High	Moderate	1. Huge overhead to set up and maintain this. 2. Small shop could maybe do it, but not a large organization. 3. Consider doing it with containers when moving to Kubernetes.
	End-User Messaging Controls	1. Use email and SMS security tools to reduce spam and phishing emails.	Reduces the organization's exposure to phishing emails which may include	High	Medium	Moderate	The following platforms reduce spam and phishing emails: 1. Proofpoint is a basic hygiene, spam, phishing, and risk-based tool. Address most
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
			ransomware attachments.				attacked users through user awareness and second factors. It automatically pulls back messages, significantly reducing the amount of spam. Consider using Knowbe4 to further reduce spam and phishing emails. 2. M365 will scrub mailboxes for malware. 3. Clearswift can make custom rules to filter spam and phishing emails. It can also tell hues and tones in images and block emails at the front door.
Protect, cont.	Web Security	1. Application vulnerabilities. 2. API security. 3. Application inputs.	Vulnerable web applications are attack vectors for ransomware.	Critical	Medium	Moderate	1. API-based malware scanning engine can take in files and send them to a malware scanning engine. 2. BlueHexagon is super fast, easy to install, and super accurate. It will scan everything and see things going out in platforms without EDR. 3. Zscaler is for client traffic, while ZPA is for most proxy web traffic. Zscaler private access simulates VPN to get to internal resources. 4. CISCO Umbrella identifies newly-registered domains and C&C servers. It points all DNS servers to CISCO Umbrella, catching malware on newly registered domains.

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
Detect Detect, cont.	EDR Detection Capabilities	1. Software and agents on user devices and servers to detect and contain ransomware while alerting employees of the threat.	EDR will detect and contain ransomware at the endpoint and prevent it from spreading. EDR is now being considered as a requirement for cyber insurance.	Critical	Low	Moderate	1. EDR capabilities are effective in preventing attacks. 2. CounterTack is an excellent solution that stops ransomware attacks by detecting, alerting, quarantining, and preventing. It can be installed on all workstations and servers to monitor asset management for A-V, EDR, and patch management. It feeds into the security information and event management (SIEM) system and alerts if an asset lacks active software. Conducting a proof of value makes it an easy business case to justify. It takes four weeks to implement on 6000 workstations and a few thousand servers but can be bundled in a SOC solution. 3. Microsoft E5 modernizes endpoints and workstations. It defends endpoints and works well. 4. Crowdstrike has an easier rollout and works best with older operating systems. It needs a monthly patch cycle, as previous legacy AV solutions can cause problems. Crowdstrike has discovery capability and integrates with SOC for better performance on endpoints and fewer crashes. It is also easy to push out and implement.
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
							5. CarbonBlack stopped two incidents cold and costs $20/node. 6. Sentinel One has a $1 million ransomware guarantee. 7. Symantec works but is not as good as other options.
	Intrusion Prevention Systems (IPS) / Data Loss Prevention (DLP) Software IPS/DLP, cont.	IPS: Host or network-based software to detect, alert, and contain known threats. DLP: Software to prevent sensitive data from leaving the entity's network.	IPS will stop known threats based on signatures but will not stop zero-day threats or perform behavioral analysis on threats. DLP will stop known sensitive data from leaving the network, but not data encrypted by ransomware.	Low	Medium	Moderate	IPS is signature-based and only detects threats known to the software. Unfortunately, ransomware morphs. DLP is dead, but is hard to implement or replace with a product falling into the data lineage space. Consider alternatives: 1. CyberHaven will give you full visibility into the lifecycle of a document and alerts on potential wrongful access based on data repositories; it does not have to inspect data since it fingerprints and hashes the document and watches where it goes. It is easy to set up, but configuration takes time, and the program needs constant tuning. Consider integrating with M365 functions.

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
							2. Consider context-based email solutions with built-in email DLPs. They can detect sensitive information without significant tuning. 3. There are many ways to perform data exfiltrations, from using CASB to restricting Dropbox.
Detect, cont.	SOC/SIEM Alerts	1. Log analysis and event alerting for evaluating potential incidents.	Useful to look for anomalous behavior, like attempted logins which may indicate lateral movement of ransomware.	Moderate	Medium	Moderate	1. Not as effective as ransomware moves at lightning speed, so seconds matter. 2. Consider implementing a Security Orchestration, Automation & Response (SOAR). 3. Add active threat hunting.
Respond	Incident Management	1. An enhanced plan to specifically address the ransomware threat, including an extended CIRT and recovery team. 2. Ransomware pay-no-pay policies.	Key to responding to and containing ransomware incidents	Critical	Medium	Low	See "Additional Member Guidance" section
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
Respond, cont.	Incident Management, cont.	3. Communications team for internal and external communications. 4. Ties to external organizations, including support personnel and law enforcement. 5. Test the plan, including network containment decisions, communications, and pay-no-pay decisions.					
	EDR Response Capabilities	See EDR Detection Capabilities	See EDR Detection Capabilities	Critical	Low	Moderate	See EDR Detection Capabilities
	Isolation Capabilities	1. Capability of the SOC, network services, or the security team to isolate network segments and	This control is vital to containing a ransomware attack and preventing it from spreading.	Critical	Medium	Moderate	1. Ensure that the appropriate team is given blanket permission to shut down network segments, systems, and devices when they are alerted of a ransomware incident.

NIST CSF FUNCTION	CONTROL *(control/strategy)*	DESCRIPTION/ COMPONENTS	RELEVANCE	VALUE *(Value to supporting CSF function: critical, high, medium, or low)*	IMPLEMENTATION DIFFICULTY *(How challenging it is to implement this control)*	COSTS *(Order of magnitude additional costs)*	MEMBER COMMENTS / BEST PRACTICES
		devices compromised by ransomware.					
Recover	Protected Backups	1. Backups on independent media, not failover, in a separate environment. 2. Backups over multiple periods, both full and incremental.	Backups are critical to recovering non-compromised data.	Critical	Medium	Moderate	1. Focus on protecting backups using WORM technology so they cannot be written over or deleted. 2. Make sure backups are not backing up ransomware-infected systems. 3. Failover process does not ensure recovery, as data may be corrupted. 4. Recover system configurations *and* data. 5. Segregate backups from the working environment.
	Clean Environment Recovery	1. Verification of clean backups. 2. Restoral to an environment that has not been infected or cleaned of ransomware.	Restoring to devices that are infected will perpetuate the compromise of data.	Critical	High	High	1. Ensure the new environment is clean. For example, do restore to a compromised active directory environment.
	Business Continuity	1. Formal BCD/DR plans that assign responsibilities.	Key to recovering systems and business processes after ransomware				See "Additional Member Guidance" section
NIST CSF FUNCTION	**CONTROL** *(control/strategy)*	**DESCRIPTION/ COMPONENTS**	**RELEVANCE**	**VALUE** *(Value to supporting CSF function: critical, high, medium, or low)*	**IMPLEMENTATION DIFFICULTY** *(How challenging it is to implement this control)*	**COSTS** *(Order of magnitude additional costs)*	**MEMBER COMMENTS / BEST PRACTICES**
Recover, cont.		2. Periodic testing of the plan. 3. Test recovering data when entire environments are corrupted by ransomware.	has compromised a computing environment.	Critical	High	High	