Internet Policy Research Initiative

Ransomware Readiness Index:

A Proposal to Measure Current Preparedness and Progress Over Time

3 September 2021
IPRI/2021/WP/02

Rebecca Spiewak
Taylor Reynolds
Daniel Weitzner

IPRI Working Paper Series
2021

https://internetpolicy.mit.edu

Ransomware Readiness Index: A Proposal to Measure Current Preparedness and Progress Over Time

3 September 2021
MIT Internet Policy Research Initiative
Rebecca Spiewak
Taylor Reynolds
Daniel Weitzner

Abstract

Ransomware is currently one of the most pressing cybersecurity threats for enterprises. While the consequences of ransomware have been long known, both firms and governments lack critical information needed to assess progress toward meaningful resilience. In this paper, we propose a new “Ransomware Readiness Index” (RRI) based on in-depth independent analysis of recently issued United States Executive Branch policy guidance on cybersecurity and ransomware. The RRI measures the aggregate level of enterprise readiness by sector (as well as other attributes), identifies the areas most at risk, and tracks progress over time toward full implementation of recent government recommendations. The index allows organizations to privately benchmark themselves against peers and focus on areas of opportunity to better mitigate against ransomware threats. The RRI provides policymakers with critical feedback on the progress of these important control improvement efforts. We will securely compute the new index using MIT IPRI’s SCRAM platform given its ability to aggregate data without requiring organizations to disclose their own sensitive data to other firms, to government entities or even MIT researchers performing the index computation.

Acknowledgements

We would like to thank Larry Susskind, David Hong, Avi Baral, Una-May O’Reilly, and Joe Pato from MIT for their insights as we put together the index. We also want to thank all the participants in our ongoing, private SCRAM computations who provided key feedback and suggestions on the approach.

Executive Summary

Overview

With increasingly sophisticated threat actor tactics, an expansion of internet-connected services and assets, and a thriving anonymous digital currency ecosystem, the threat of ransomware both within the US and abroad remains significant. In recent years, the Biden administration has called for heightened cybersecurity measures on the part of both government agencies and private industry to protect national security interests. Despite the government's and public's growing interest in addressing cybersecurity issues, the ability to fully understand and prioritize steps to combat ransomware-related risks remains elusive. This is partially driven by a dearth of ransomware information available that could help inform where additional security support would be most beneficial. This data scarcity is largely driven by the desire for enterprise anonymity when breached by an attacker. The diversity of industries that are affected by ransomware – from healthcare firms to technology giants, local municipalities to energy infrastructure – also makes it difficult to both track and manage how well enterprises are faring against ransomware attacks.

To invest in new technologies, adjust existing security practices and craft better policies, both public and private stakeholders require meaningful metrics to track progress against ransomware over time. In this vein, this proposal lays out the foundations for control areas to track and measure through a set of **Ransomware Readiness Indices (RRI)** by leveraging the secure multi-party computation platform called **SCRAM (Secure Cyber Risk Aggregation and Measurement)** that was developed by a team from MIT's Internet Policy Research Initiative (IPRI) and Computer Science and Artificial Intelligence Laboratory (CSAIL).

Security Controls Benchmarking: General Approach

To build the RRI, data will be collected from organizations through MIT's SCRAM platform (scram.mit.edu). SCRAM generates metrics in an aggregated fashion by performing computations on encrypted data collected from participating stakeholders. By using this platform, the data is protected, so participating organizations can remain at ease regarding the sensitive nature of the data.

Through an extensive independent review and analysis, ransomware controls were defined and codified by MIT policy and cybersecurity researchers. These controls are grounded by the guidance in the White House Executive Order (EO) and related White House Memo issued in Spring 2021. Participating entities will be asked to rate their organization's level of control maturity (i.e., adoption) across this specific set of ransomware-related controls. Below is a high-level depiction of the overall approach:

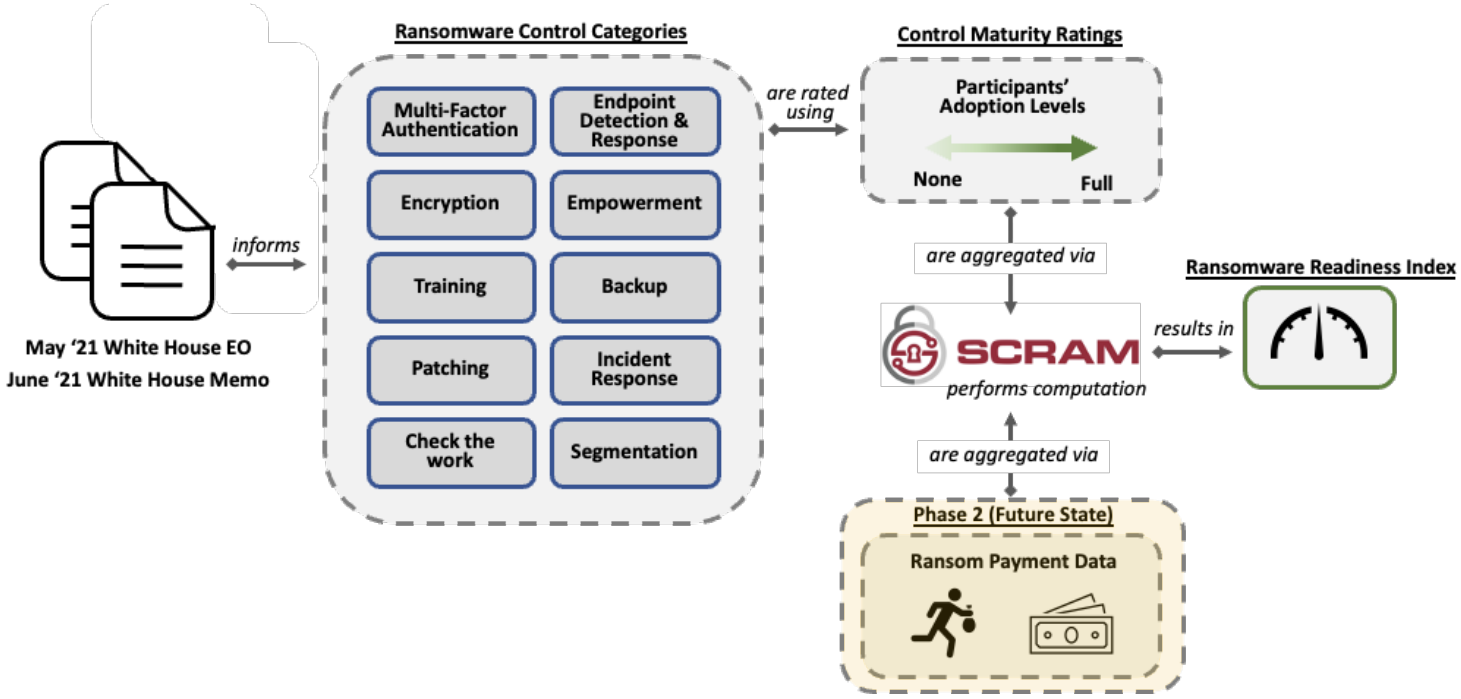

Figure 1: Ransomware Readiness Index Approach

Security Controls Benchmarking: Phase 1 Output

In establishing the RRI, our initial aim is to understand the level of readiness against ransomware and the collective areas of greatest risk to our critical infrastructure. In the longer-term, the RRI will highlight how well entities are managing their risk over time. Trends related to ransomware techniques, new vulnerabilities and the ransomware market writ-large can then be analyzed in the context of the information provided through the RRI.

The output of the computation will include an aggregate view of security readiness across the ten ransomware control categories portrayed in the graphic above, as well as across twenty-two more granular controls referenced in the Biden Administration EO and Memo. This information will be further segmented by company size and industry, creating a set of highly curated RRIs with anonymous data.

Ransomware Loss Data Benchmarking: Phase 2 Output

While the initial focus of the RRI is security controls maturity data, planned future-state output will concentrate on the monetary side of the ransom demand itself. The ability to collect data from enterprises securely and anonymously places SCRAM in a unique position to collect sensitive yet critical questions related to the frequency and amount of ransom demanded, as well as whether the ransom was ultimately paid out to the attackers. We believe the economy

and ecosystem that enables threat actors to both solicit and receive ransom is worthy of dedicated analysis, especially given the lack of current transparency on this topic.

Stakeholder Participation

The greater the number of RRI participants, the more valuable this data will be for organizations. If your organization is interested in hearing more about our ongoing RRI effort, or participating in an upcoming computation, please reach out to scram@mit.edu. For more information, a more detailed proposal is documented in the remainder of this whitepaper. The proposal discusses the relevant historical context, a more in-depth look at which controls are measured via the RRI, and the team's upcoming involvement with local municipalities which includes providing security control resource recommendations.

Introduction: The threat of ransomware against US critical infrastructure

Ransomware is currently one of the most pressing threats against diverse but essential infrastructure within the US. Security teams have concentrated on securing their environments and enhancing their operational processes to defend against these attacks for years, but the recent frequency and change in tactics by perpetrators have both increased the potential damage from incidents, as well as the attacker's leverage over their victims [1] . We need a better understanding of the ransomware market and ecosystem in combination with industry readiness in order to curb this trend.

Historical context: Major ransomware milestones

To better mitigate the harm caused by ransomware attacks, it is important to contextualize the associated threat landscape and the impact on critical sectors within the US and abroad. In 2017, the Petya attack – and its subsequent, more devastating NotPetya faux-ransomware counterpart – represented a major transition point for cyber threats given the size, scale and efficacy of the events. The attacks impacted banking, public transit, energy and key enterprises across Europe, taking advantage of unpatched Windows machines by building off of the endpoint encryption techniques from prior WannaCry / EternalBlue attacks [2] [3]. NotPetya alone is estimated to have cost $10 billion in damages [2]. Most significantly, these attacks laid bare not only the vulnerability of critical sector infrastructure, but also how unprepared private enterprises and government entities were to recognize and address those security weaknesses in the context of sophisticated threat actors motivated by both financial gain and large-scale disruption of specific nation-states.

While the trend of targeted ransomware attacks against critical sectors is widely recognized, the underlying details around attack specifics remains opaque. In October 2020, threat actors specifically focused on compromising hospitals through ransomware attacks, taking advantage of the weak negotiation leverage hospitals had during the COVID-19 crisis [4]. CISA, the FBI, and the Department of Health and Human Services issued a joint advisory notice, warning healthcare organizations specifically about Ryuk and Conti ransomware and how to better secure their networks against these particular threats [5]. In 2021 alone, critical sector entities that were targeted include global meat producer JBS [6], the Colonial Pipeline [7], and the Apple product manufacturer Quanta – a company that successfully refused to pay $50 million in ransom, but at the cost of leaked trade secrets [8].

The latest trend of cybersecurity exploits, classified under the category of software supply chain attacks, poses one of the greatest threats to both industry and government networks across the globe given its ability to remain undetected using traditional security controls. The attack on SolarWinds discovered in late 2020 demonstrated that if a software update can be compromised, malicious code can be pushed out to the company's third party client-base and avoid detection, serving as a large-scale launchpad for unrestrained access and future attacks

[9]. While the SolarWinds hack was not ransomware, it served as the precursor to the ransomware attack on the software company Kaseya in July of 2021. The Kaseya attackers, who requested $70 million in ransom in exchange for a universal decryptor, relied on a zero-day exploit of the company's remote managed services to take offline more than 1,500 companies [10]. Ultimately, given the noted malicious actor incentives and expertise, immense attack scale and frequency, and calamitous impact of these ransomware attacks, it is essential for researchers to provide methodologies and tools offering greater transparency in this space to better inform key business and policy-making decisions.

Historical context: US Government response

In reaction to the high-profile ransomware attacks discussed above, stakeholders both within industry and the government have called on policymakers to prioritize this security issue. The US government has taken action through various recommendation and policy-oriented mechanisms:

- **CISA / MS-ISAC / NGA / NASCIO Recommended Actions (July 2019)**
  CISA and several organizations issued a set of recommendations in July 2019 to increase resilience against ransomware. These recommendations included backing up systems, reinforcing basic cybersecurity awareness and education, and revisiting/refining cyber incident response plans [11].

- **CISA 2019 Insights (Aug 2019)**
  In 2019, the United States Cybersecurity and Infrastructure Security Agency published recommendations to defend against ransomware via its CISA Insights publication. The one-page document provided five steps to secure systems, five steps to take once hit, and five actions to secure the environment going forward. The CISA Insights document also pointed to the CISA Resource Page on ransomware [12].

- **Cyberspace Solarium Commission (CSC) Report (Mar 2020)**
  Through the CSC established via the John S. McCain National Defense Authorization Act in 2019, the US government issued strong, specific action-oriented recommendations to build stronger defenses while shifting misaligned existing incentive structures. Recommendations focused on creating new cybersecurity organizational structures with greater authority, providing better mechanisms for measurement and transparency regarding efficacy, and implementation costs to motivate deterrence [13].

- **CISA 2020 Ransomware Guide (Sept 2020)**
  In 2020, CISA published a ransomware guide that laid out best practices for ransomware prevention and provided guidance for incident response [14].

- **US White House Executive Order on Improving the Nation's Cybersecurity (May 2021)**

In May 2021, the White House issued an executive order directing the federal government to secure all federal information systems with multi-factor authentication, endpoint detection and response (EDR), encryption, and by having a skilled and empowered security team [15].

- **US White House Memo (June 2021)**
  The White House sent out a memo to firms across the country recommending steps they could take to defend against ransomware. These build on top of the recommendations in the May 2021 Executive Order of multifactor authentication, endpoint detection and response, encryption, skilled & empowered security team. The additional items include backing up systems, patching systems promptly, testing the incident response plan, checking the security team's work, and segmenting networks [16].

- **NIST Draft Profile (June 2021)**
  In June 2021, NIST released a preliminary draft cybersecurity framework profile for ransomware risk management. The framework categorizes controls in NIST's five categories (identify, protect, detect, respond, recover). The document also maps specific controls from the NIST CSF to ISO/IEC 27001:2013 and NIST SP 800-53 [17].

- **Ransomware and Digital Extortion Task Force (June 2021)**
  Addressed to all US prosecutors, the associated memo created the Ransomware Taskforce with aims to empower legal stakeholders and hold threat actors accountable for ransomware attacks [18].

These documents provide a range of steps organizations can take to defend against ransomware attacks. However, calls to action in this policy space are relatively recent given the shift in threat actor tactics and attack frequencies. The government is also relying on data associated with large-scale, often highly public breaches to make their recommendations, rather than from a trove of well-established, standardized, available data sources. This proposal aims to close this gap to support policymaking that can ultimately help private industry and governments better protect against ransomware.

The challenge of progress tracking: "You can't manage what you can't measure"

While there is a general consensus among the policy and security communities regarding the importance of ransomware defenses, there is no agreed-upon method for gauging ransomware preparedness and no systematic collection of data on defenses to track progress toward resilience over time. If the popular business axiom of "you can't manage what you can't measure" holds true, then managing the steady progression of enhancing security defenses against ransomware will pose a significant challenge for policymakers and organizations alike.

Reporting and anonymity

A significant barrier to understanding current areas of greatest weakness against the threat of ransomware is the reluctance of organizations to disclose a breach. For a private organization, detailing the nature of a cybersecurity incident often comes with known risks. First, companies face reputational risk when revealing their network was indeed compromised [19]. For example, despite the transparency provided by UK telecommunications company TalkTalk after their October 2015 cyber attack, the company lost over 100,000 customers due to a general lack of trust [19]. Firms may worry about falling stock prices [20], loss of monetary compensation, or employees may fear losing their job [21]. After the Capital One breach was discovered in July 2019, RBC Capital Markets analyst Jon Arfstrom stated, upon seeing falling stock prices, “We worry about longer term reputational damage and also the potential for political and regulatory actions, including penalties” [22].

On this note, companies do often feel that reporting a breach can lead to additional regulatory scrutiny and subsequent costly changes to technology and operations, largely without additional resources or government support; despite the inaccuracy in some of these assumptions, this in turn can disincentivize full transparency within the security space [23] [24]. Specific to ransomware attacks, the FBI does not condone rewarding attackers; paying ransom to cybercriminals continues to drive these nefarious acts and is noted as a key contributor to the growing ransomware market [25]. As a result, organizations often do not reveal if ransom was paid out, either directly or through a cybersecurity insurance firm or other third party [26].

Most importantly, firms are reticent to reveal specifics regarding vulnerabilities, failed controls or weak security procedures. While understanding common weaknesses amongst organizations could help the government provide more robust support, firms do not wish to put a proverbial target on their backs, visible to a sophisticated hacker community [27]. Overall, these combination of factors make it difficult to cultivate meaningful metrics to help inform cybersecurity policy and governmental support.

Inconsistent measurements

We need an understanding of our current security state, the ability to identify security gaps, and a method for tracking progress toward ransomware resilience over time in order to manage the economy’s move toward better ransomware preparedness. Aside from a reluctance from companies to disclose data regarding ransomware incidents and losses, progress in this area has been hampered in other ways. There is a general lack of systematic data collection on defense posture. This is not only driven by a lack of a mandate, but an inconsistent understanding of what specific data would be most helpful, as well as from where the most robust data sources can be derived [28]. In addition, competing control frameworks and profiles exist, making data harmonization a challenge. For example, while security control frameworks such as the NIST Cybersecurity Framework (CSF) [29] and the 18 CIS Controls [30] are well-known and widely leveraged, the purpose, extent and method of usage varies a great deal based on the industry-alignment and size of an enterprise.

Proposal: Creation of Ransomware Readiness Indices (RRI)

Thankfully, there are signs on the horizon that these data challenges can be meaningfully addressed. In August 2021, the US National Cyber Director Chris Inglis argued for the creation of a new office in the Department of Homeland Security, with a focus on cyber statistics. This office would be empowered with the authority to collect cyber threat and loss data in partnerships with the private sector [31]. Internationally, groups such as the Organisation for Economic Co-operation and Development (OECD) are working to develop new cyber statistics frameworks that would be comparable across countries. These efforts will play an important role in helping to move progress forward, and serve as foundational for the successful implementation of ransomware-specific metrics made possible via MIT's multi-party computation platform, SCRAM [32].

We propose an action-oriented solution to the longstanding security data challenges discussed via the creation of industry-specific Ransomware Readiness Indices (RRI). RRI is built on a standardized set of controls informed by the recent May 2021 US Executive Order and June 2021 White House Memo [15] [16]. The RRI set will support industry and economy-wide benchmarks for ransomware preparedness that firms can use internally to compare their own progress against others in their industry and inform their own security investment decisions. The RRI can also be extended to gather information on ransomware losses in a secure and private way. With these new statistics emerging from the RRI, policymakers will have additional tools to inform policy and address issues with overall ransomware market incentives through different policy and industry levers.

Foundational approach and stakeholder benefits

The RRI large-scale data collection will run on MIT's SCRAM platform (scram.mit.edu). SCRAM generates aggregate statistics by performing computations on encrypted data from multiple parties; **data is never disclosed by any of the data contributors thanks to the security provided by the SCRAM platform**. Currently, the SCRAM platform is already in use for benchmarking the security defenses of large firms and calculating cyber security risk given a common set of incident and control parameters.

The immediate benefit of the SCRAM platform to participating firms is clear: There is comfort in the ability to compare an internally-defined security posture against applicable security benchmarks articulated via the RRI -- remarkably, this is without any required ransomware incident disclosure to government entities, industry partners, third parties providers, or even MIT. Firms will be able to produce comparisons to peer groups that can then be used internally to justify resource allocations and satisfy security-related requests from corporate boards. Policy-makers will also be able to follow industry trends built on sensitive data without the need to store and protect the sensitive data from individual firms. Over time, we hope to further

contextualized results against more granular threat and loss data to drive action-oriented solutions.

In establishing the RRI, our initial aim is to understand the following:

1. **Level of readiness:** How prepared are firms in a given sector against ransomware based on their adoption of high-impact security defenses?
2. **Collective areas of greatest risk**: Which defensive control categories have the lowest level of maturity in the context of ransomware, leading to heightened critical infrastructure risk?
3. **Maturity progress over time:** How are high-impact defense adoption efforts progressing over time?

RRI Creation: Index profile structure

Through a White House Executive order and subsequent White House Memo issued in the Spring of 2021, the US Administration called on firms to take specific steps to respond to ransomware threats [15] [16]. This proposal provides a typology of ransomware security defenses that directly aligns with ten specific government control category recommendations called out by the current US administration via these notifications.

The typology will form the basis of several large-scale computations on the SCRAM platform running over encrypted data that is never disclosed by the contributors. We will produce benchmarks by sector, geography, and relevant size of the organization. Each RRI serves as a point-in-time snapshot of critical ransomware-relevant control adoption, and can be analyzed in the context of additional data sources, such as those related to threat intelligence and the ransomware digital currency economy. The information below details both the controls the RRI tracks, as well as how control maturity is articulated.

The RRI profile consists of twenty-two controls across the ten categories identified in the White House Memo, as shown in the figure below. While each control item is mapped back to a control articulated within the NIST and CIS frameworks, each control is ultimately aligned with the White House Memo in order to better ground maturity ratings in the context of ransomware rather than security more holistically.

Category	Control	Not Implemented	Partially Implemented	Largely Implemented	Fully Implemented
1. MFA	1a. Deploy multi-factor authentication across the enterprise				
2. EDR	2a. Deploy an endpoint detection and response (EDR) system / host-based IPS agent				
	2b. Hunt for malicous activity				
3. Encryption	3a. Encrypt data in transit				
	3b. Encrypt data at rest				
4. Empowerment	4a. Remove barriers to sharing				
	4b. Receive external threat intelligence				
5. Training	5a. Evaluate skills				
	5b. Deliver regular training				
6. Backup	6a. Perform regular backups of systems				
	6b. Test backup data				
	6c. Protect backups				
	6d. Store backups in offline location				
7. Patch	7a. Deploy updates and patches in a timely manner				
	7b. Implement a centralized patch management system				
	7c. Apply patches using a risk-based approach				
8. Incident response	8a. Codify an incident response plan				
	8b. Test your incident response plan				
	8c. Maintain your incident response plan				
9. Check the work	9a. Establish an external penetration testing program				
	9b. Perform red team exercises				
10. Segment	10a. Adopt network segmentation to ensure isolation of critical systems in an attack				

Figure 2: Control Maturity Assessment for the RRI

Creating control categories

The White House Memo [16] further narrowed the focus of the government's guidance, with recommendations to strengthen security controls related to ransomware specifically. First, the Memo urged business leaders to implement five high-impact best practices highlighted in the Executive Order. The first five categories below align directly to those high-impact areas. The remaining five are called out in the Memo as essential security practices that can reduce both the probability of a successful attack and the extent of the potential impact of ransomware once successfully executed [16]. Below, we have detailed a more in-depth alignment between the

White House's calls to action and the RRI categories. We have also mapped these categories back to several cybersecurity control frameworks for reference purposes.

Category 1: Multi-Factor Authentication (MFA)

The White House Memo calls out MFA as a high-impact area, noting "passwords alone are routinely compromised" [16]; the language within the RRI control directly ties to this Memo recommendation. The control is also mapped to the NIST CSF [29], as well as the CIS Controls versions 7.1 [32] and 8 [30] as best as possible.

RRI	**Control 1a: Deploy Multi-Factor Authentication across the enterprise**
NIST CSF	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
CIS 18 v8	5.2 Use Unique Passwords 6.5 Require MFA for Administrative Access
CIS 20 v7.1	16.3 Require Multi-factor Authentication 11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions

Category 2: Endpoint Detection & Response (EDR)

The White House Memo notes two capabilities under the heading of EDR -- namely, "to hunt for malicious activity on a network and block it" [16]. With regard to Federal Civilian Executive Branch (FCEB) Agencies, the original White House Executive Order goes a bit farther, stating agencies, "shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response" [15].

In this vein, we acknowledge that endpoint detection and response can speak to both a technical implementation (i.e., an EDR tool deployed within an enterprise's network) and an operational capability (i.e., the act of detecting and responding to cyber events identified on an endpoint). It is important to note that each interpretation cannot be looked at independently; effective operational capabilities often rely on robust security tools, and vice versa. The two RRI controls under the EDR category attempt to hit upon both aspects of EDR.

Keeping these recommendations in mind, a referential mapping to control frameworks maintains a dual approach to detection and response via both technical implementations and operational capabilities as best as possible:

RRI	**Control 2a: Deploy an endpoint detection and response (EDR) system / host-based IPS agent** **Control 2b: Hunt for malicious activity**
NIST CSF	DE.CM-1: The network is monitored to detect potential cybersecurity events
CIS 18 v8	10.5 Enable Anti-Exploitation Features 13.1 Centralize Security Event Alerting 13.7 Deploy a Host-Based Intrusion Prevention Solution
CIS 18 v7.1	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies 6.6 Deploy SIEM or Log Analytic tool 13.5 Monitor and Detect Any Unauthorized Use of Encryption

Category 3: Encryption

The White House Memo states that encryption is essential to reducing the threat of ransomware because, "if data is stolen, it is unusable" [16] The Executive Order provides more granular detail, specifying encryption should be applied to data both at rest and in transit [15]. Both the RRI's articulated controls and the mapping to each framework are relatively clear-cut:

RRI	**Control 3a. Encrypt data in transit** **Control 3b. Encrypt data at rest**
NIST CSF	PR.DS-2: Data-in-transit is protected PR.DS-1: Data-at-rest is protected
CIS 18 v8	3.10 Encrypt Sensitive Data in Transit 3.11 Encrypt Sensitive Data at Rest
CIS 20 v7.1	14.4 Encrypt All Sensitive Information in Transit 14.8 Encrypt Sensitive Information at Rest

Category 4: Empowerment

The Memo speaks to enabling "the existence of a skilled, empowered security team," calling out patching, as well as sharing and infusing threat intelligence directly into defense capabilities [16]. The Executive Order also references the ability to share intelligence both within and across different government agencies by removing bureaucratic barriers [15]. Because patching is a separate control category, we emphasized empowerment on the threat intelligence side rather than from a patch management perspective, to reduce redundancy. As a result, the control framework mappings focuses on information sharing and related incident handling in the context of empowerment.

RRI	**Control 4a. Remove barriers to sharing** **Control 4b. Receive external threat intelligence**
NIST CSF	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources 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)
CIS 18 v8	17.1 Designate Personnel to Manage Incident Handling 17.3 Establish and Maintain an Enterprise Process for Reporting Incident
CIS 20 v7.1	19.2 Assign Job Titles and Duties for Incident Response 19.6 Publish Information Regarding Reporting Computer Anomalies and Incidents

Category 5: Training

While training is not explicitly referenced in the Memo, we felt that the "empowerment" category above should be interpreted to include upskilling. Without an up-to-date knowledge-base and the appropriate set of skills to accompany this education, it would be difficult for the authors to consider a team or organization adequately empowered to protect their firm against ransomware. This is true both for cybersecurity specialists, as well as general employees who have a responsibility to protect their firm where they can. The Executive Order also alludes to training to handle proper information sharing and collaboration through the Fed RAMP program [15].

Bolstering the importance of this category, the Biden administration held a Cybersecurity Summit in August of 2021 with industry leaders across various sectors, including technology, finance, energy, and cybersecurity insurance [34]. Companies publicly committed to further supporting the nation's cybersecurity goals, with many dedicating resources to training. IBM committed to training 150K individuals in cybersecurity over the course of the next three years, while Girls Who Code launched a micro-credential program for groups typically marginalized from access to successful technology career paths [35].

RRI	**Control 5a. Evaluate skills** **Control 5b. Deliver regular training**
NIST CSF	PR.AT-1: All users are informed and trained PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
CIS 18 v8	14.1 Establish and Maintain a Security Awareness Program 14.9 Conduct Role-Specific Security Awareness and Skills Training

CIS 20 v7.1	17.1 Perform a Skills Gap Analysis 17.2 Deliver Training to Fill the Skills Gap

Category 6: Backup

The White House Memo is very specific with regard to maintaining backups, given the relevance to reducing the leverage a threat actor could have against an organization in the event of a ransomware attack. The Memo recommends for firms to "Backup your data, system images, and configurations, regularly test them, and keep the backups offline" [16]. The RRI pulls directly from these explicit guidelines.

RRI	**6a. Perform regular backups of systems** **6b. Test backup data** **6c. Protect backups** **6d. Store backups in offline location**
NIST CSF	PR.IP-4: Backups of information are conducted, maintained, and tested
CIS 18 v8	11.1 Establish and Maintain a Data Recovery Process 11.2 Perform Automated Backups 11.3 Protect Recovery Data 11.4 Establish and Maintain an Isolated Instance of Recovery Data 11.5 Test Data Recovery
CIS 20 v7.1	10.1 Ensure Regular Automated Backups 10.2 Perform Complete System Backups 10.3 Test Data on Backup Media 10.4 Protect Backups 10.5 Ensure All Backups Have at Least One Offline Backup Destination

Category 7: Patching

Untimely patching as a result of poor technology hygiene can provide unwanted opportunities for threat actors to infect a network and spread ransomware. Patching is a key preventative measure, with the Memo stating that timely patches should ideally be applied across all relevant infrastructure using a risk-based approach via centralized tooling [16]. The RRI separates out timeliness, centralization and risk into three distinct controls to best align with these government recommendations.

RRI	**7a. Deploy updates and patches in a timely manner** **7b. Implement a centralized patch management system** **7c. Apply patches using a risk-based approach**
NIST CSF	DE.CM-8: Vulnerability scans are performed PR.IP-12: A vulnerability management plan is developed and implemented
CIS 18 v8	7.3 Perform Automated Operating System Patch Management 7.4 Perform Automated Application Patch Management
CIS 20 v7.1	3.4 Deploy Automated Operating System Patch Management Tools 3.5 Deploy Automated Software Patch Management Tools 10.5 Ensure All Backups Have at Least One Offline Backup Destination

Category 8: Incident response

Robust incident response capabilities are emphasized in both the White House Memo and Executive Order. It is well-understood that even if highly sophisticated preventative security measures are implemented, at some point organizations will fall victim to an attack. As the saying within the security community goes, "it's not a matter of 'if', but 'when.'" As such, the White House Memo underscores the importance of testing an incident response plan to understand current state gaps and iteratively improve based on the outcomes [16]. The RRI takes this a step farther, and includes the act of both creating and maintaining this plan, in addition to testing.

RRI	**8a. Codify an incident response plan** **8b. Test your incident response plan** **8c. Maintain your incident response plan**
NIST CSF	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed PR.IP-10: Response and recovery plans are tested
CIS 18 v8	17.4 Establish and Maintain an Incident Response Process 17.7 Conduct Routine Incident Response Exercises
CIS 20 v7.1	19.1 Document Incident Response Procedures 19.7 Conduct Periodic Incident Scenario Sessions for Personnel

Category 9: Checking the work

This category ties back to the Memo's recommendation for security teams to use third-party methods of independently assessing the security of an enterprise [16]. While pen testers are directly noted as an option, the RRI generalizes to include other equally effective methods of

assessing security from an external perspective in a threat-based manner. This is reflected in our mapping to other control frameworks as well.

The Executive Order also notes the importance of pen testing in the context of vendors, stating NIST, “shall publish guidelines recommending minimum standards for vendors’ testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing)” [15].

RRI	**9a. Establish an external penetration testing program** **9b. Perform red team exercises**
NIST CSF	ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
CIS 18 v8	18.1 Establish and Maintain a Penetration Testing Program 18.2 Perform Periodic External Penetration Tests
CIS 20 v7.1	20.2 Conduct Regular External and Internal Penetration Tests 20.3 Perform Periodic Red Team Exercises

Category 10: Segmenting

Segmentation is a key control category aimed at preventing the spread of ransomware once a part of the network is infected. The Memo recommends network segmentation from a business continuity standpoint, given the transition from data theft to business disruption in a ransomware scenario [16]. The ability to isolate critical infrastructure in the event of an attack is a notable priority for the US government. With regard to critical software, the White House Executive Order also references the importance of segmentation [15].

RRI	**10a. Adopt network segmentation to ensure isolation of critical systems in an attack**
NIST CSF	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
CIS 18 v8	113.12 Segment Data Processing and Storage Based on Sensitivity 13.4 Perform Traffic Filtering Between Network Segments
CIS 20 v7.1	14.1 Segment the Network Based on Sensitivity 12.2 Scan for Unauthorized Connections across Trusted Network Boundaries

Maturity Rating Methodology and Participant Expectation

Participating enterprises will each rate their organization's maturity (i.e., adoption level) of the controls articulated above. Please refer to Appendix A to view the full RRI Control Maturity Rating template. The maturity rating is based on the following scale:

1. Not implemented
2. Partially implemented
3. Largely implemented
4. Fully implemented

We recognize that the control maturity levels, ranging from "Not Implemented" to "Fully Implemented," can be interpreted in a variety of ways. Implementation level should not be based on the organization's progress vs. the *planned* end-state, but rather an implementation level with respect to the *ideal* end-state recommended by frameworks and regulators. When rating maturity, an organization should ask itself, "If I had unlimited time, expertise and resources, what would the end-state for this control's implementation look like?" The responses will be based on this perspective.

Maturity ratings are defined as follows:

- **Not Implemented:** The described control does not exist within your organization in any form.
- **Partially Implemented:** Considered 50% or less based on one or more of the following dimensions:
    - Network surface area: The control is implemented on some parts of your network but not others (e.g., EDR is deployed on Windows endpoints but not Linux, data is encrypted locally but not in the cloud)
    - User adoption: The control has been adopted by only a portion of end-users (e.g., MFA is used on 50% or fewer employee cell phones, cybersecurity training is provided to only a small subset of employees)
    - Capabilities: The control is implemented in a fashion that does not fully utilize the security capabilities as expected (e.g., patching is done in a manual fashion once a quarter, whereas weekly automated patching is preferred)
- **Largely Implemented:** Considered 80% or less based on the same dimensions described above.
- **Fully Implemented:** 95% implementation or higher. There is an understanding that 100% control implementation is not always realistic or verifiable.

Future State Efforts: Ransomware Loss Data

We believe that beyond security controls data, SCRAM's secure data collection and computation capabilities provides additional opportunities to aggregate and assess

cybersecurity risk. Specifically, a diverse array of stakeholders, including cybersecurity specialists, regulators and vendors, are interested in the ability to better quantify and manage cybersecurity risk in the context of monetary losses, and much of this data remains opaque. However, we acknowledge that it is often difficult to reach a consensus on the definition of "financial loss" for a cybersecurity breach; for example, how does one quantify the loss experienced due to the exposure of sensitive data, or overall damage of reputational risk?

In the case of ransomware threats, we have a real opportunity to analyze a relatively well-defined risk by focusing on the ransom dollar amount and data availability aspects of the incidents. By collecting and analyzing accurate and timely information on ransom payments, robust policies and products can be put in place to help stifle the continued growth of the ransomware economy.

In Phase 2 of the RRI, organizations will be asked to provide information on the following items:

- The number of attempted ransomware incidents an organization has experienced
- Whether ransom was paid, either by the organization directly or through a third party (e.g., insurance provider)
- The aggregate sum of ransom paid by an organization over a set period of time
- The average amount of time it took for an organization to return to normal operations after a successful ransomware attack

Case Study: Municipalities across a state

Municipalities are at a heightened state of risk, given the increase in frequency of targeted ransomware attacks against networks related to cities and towns, services such as water and waste management, and public schools. The prevalence of these threats, paired with the lack of resources to thwart attacks, make municipalities an important constituency that could benefit from RRI benchmarking to identify and address security gaps. MIT's IPRI will work with local municipalities to pilot the RRI, provide benchmarks on ransomware preparedness for decision makers at the local level, and help municipalities identify resources to address their own gaps.

We are planning to run a municipality data aggregation computation in Fall 2021 with a large number of local governments.

What municipalities will receive

Participating municipalities will receive a set of aggregated benchmarks they can use to compare with their own security posture without having to disclose their information to anyone.

Private benchmarking tools

Control adoption across the state	Control adoption in the region	Control adoption by similar-sized municipalities

+

Resources to address identified gaps

Access to free or low-cost security resources	Identification of applicable products and services

Timeline

Stage 1: Outreach (October 2021)
In the first stage, MIT's IPRI will hold a series of virtual information sessions with municipal leaders to let them know about the project, explain how the technology allows us to aggregate without disclosure, and get feedback on our approach. We will work with state-wide and national groupings of municipalities to raise awareness of the pilot. The outreach will begin in September 2021.

- Hold series of virtual "information sessions" where city managers and IT specialists can participate and ask questions
- Work with state-wide groupings of municipalities to raise awareness of the pilot
- Sign up municipalities to participate

Stage 2: Prepare for the computation (November 2021)
In stage 2, we will work with the municipalities as they prepare their own internal data and get it ready to put into the data template. We will also do a practice run using synthetic data to give participants exposure to the platform and how it works. Finally, we will continue our outreach to municipalities during this time.

- Finalize the data input template
- Schedule a practice run through with firms
- Continue outreach

Stage 3: Computation (end of November 2021)
In stage 3, we will schedule the computation to be run over a set period of time. Participating municipalities will upload their encrypted data via the SCRAM website during the prescribed period for the aggregation computation. At the end of the data entry period, we will combine the encrypted data and run the computation to produce the aggregated results.

- Launch and run the computation period

Stage 4: Workshop on results (January 2022)
For the next stage, we will take the results of the computation and hold a workshop with all the participants to discuss the results - highlighting areas of general strength and others that need improvement across the group. Participating municipalities will be able to benchmark themselves against the entire state, other municipalities of similar size, and potentially the region. The RRI will help us identify gaps, but we will also provide municipalities with guidance on each of the categories of how to boost defenses in a cost-effective way. We will gather options on steps municipalities could take on each category along with estimated pricing from vendors, equipment needs, and estimated staff requirements of the municipalities.

- Workshop focused on results and potential solutions to bring up lagging areas
- Focused advice and options for each of the categories that municipalities can use to improve their own security. The workshop will provide a range of options for each category, including free or low-cost resources for relevant control capabilities.

Stage 5: Schedule follow up computation for a future quarter
For the final stage, we will schedule a follow up computation for a future quarter in order to track progress of the group over time using the RRI to gauge ransomware preparedness. Future computations could also produce benchmarks for different states and expand the number of participants for each size category.

- Schedule a follow up computation

Conclusion

Through the RRI, our goal is to provide greater transparency into the current state of cybersecurity readiness against ransomware, leveraging the US government's 2021 recommendations as a set of firm foundational expectations. Companies and local governments will gain a better understanding of where they stand in terms of security, both generally and within their sector without the need to forgo anonymity, hire costly consultants, or maintain a dependency on particular tooling or services. This will ultimately enable companies to pinpoint strengths and weaknesses, and adjust their security investment spending accordingly.

In addition, our hope is for the RRI to be used to inform policy and federal resources. Once launched, the RRI effectively can serve as a "trailing check" on how well particular policies have worked once implemented. The government can then choose to adjust policies, regulations, training, and spending accordingly.

While we are currently working with local municipalities, our next area of focus is within various private sector categories, including finance, insurance, and technology. If you are interested in joining a computation in 2021 or early 2022, please reach out to scram@mit.edu.

Bibliography

[1] “Why ransomware attacks are on the rise — and what can be done to stop them,” *PBS NewsHour*, Jul. 08, 2021. https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them (accessed Aug. 27, 2021).

[2] L. H. Newman, “A Scary New Ransomware Outbreak Uses WannaCry’s Old Tricks,” *Wired*. Accessed: Jul. 26, 2021. [Online]. Available: https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/

[3] “The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED.” https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed Feb. 11, 2021).

[4] D. Goodin, “Advisories: ‘Brazen’ Russian ransomware hackers target hundreds of US hospitals,” *Ars Technica*, Oct. 29, 2020. https://arstechnica.com/information-technology/2020/10/us-government-warns-of-imminent-ransomware-attacks-against-hospitals/ (accessed Jul. 27, 2021).

[5] “Ransomware Activity Targeting the Healthcare and Public Health Sector | CISA.” https://us-cert.cisa.gov/ncas/alerts/aa20-302a (accessed Jul. 27, 2021).

[6] D. Goodin, “Shortages loom as ransomware hamstrings the world’s biggest meat producer,” *Ars Technica*, Jun. 01, 2021. https://arstechnica.com/gadgets/2021/06/ransomware-striking-the-worlds-biggest-meat-producer-threatens-shortages/ (accessed Jul. 27, 2021).

[7] S. Morrison, “The FBI recovered most of Colonial Pipeline’s ransom, but the ransomware threat remains,” *Vox*, May 10, 2021. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices (accessed Jul. 27, 2021).

[8] T. C. Illinois, “The 10 Biggest Ransomware Attacks of 2021.” http://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php (accessed Jul. 27, 2021).

[9] I. J. Canales Katie, “The US is readying sanctions against Russia over the SolarWinds cyber attack. Here’s a simple explanation of how the massive hack happened and why it’s such a big deal,” *Business Insider*. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 (accessed Jul. 27, 2021).

[10] D. Goodin, “Up to 1,500 businesses infected in one of the worst ransomware attacks ever,” *Ars Technica*, Jul. 06, 2021. https://arstechnica.com/gadgets/2021/07/up-to-1500-businesses-infected-in-one-of-the-worst-ransomware-attacks-ever/ (accessed Jul. 27, 2021).

[11] “CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks,” *Department of Homeland Security*, Jul. 29, 2019. https://www.dhs.gov/news/2019/07/29/cisa-ms-isac-nga-nascio-recommend-immediate-action-safeguard-against-ransomware (accessed Aug. 27, 2021).

[12] “CISA Insights: Ransomware Outbreak | CISA.” https://us-cert.cisa.gov/ncas/current-activity/2019/08/21/cisa-insights-ransomware-outbreak (accessed Aug. 27, 2021).

[13] “CSC Executive Summary.pdf,” *Google Docs*. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view?usp=embed_facebook (accessed Aug. 27, 2021).

[14] “Ransomware Guide | CISA.” https://www.cisa.gov/publication/ransomware-guide (accessed Feb. 11, 2021).

[15] “Executive Order on Improving the Nation’s Cybersecurity,” *The White House*, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed Jul. 28, 2021).

[16] “H-ISAC TLP White Threat Bulletin: White House Memo to Protect Against The Threat of Ransomware June 3, 2021 | AHA.” https://www.aha.org/h-isac-reports/2021-06-03-h-isac-

tlp-white-threat-bulletin-white-house-memo-protect-against-threat (accessed Aug. 27, 2021).
[17] W. Barker, K. Scarfone, W. Fisher, and M. Souppaya, “Cybersecurity Framework Profile for Ransomware Risk Management (Preliminary Draft),” National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8374 (Draft), Jun. 2021. Accessed: Aug. 27, 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8374/draft
[18] C. Porterfield, “Department Of Justice Creates New Task Force To Take On Ransomware Attacks,” *Forbes*. https://www.forbes.com/sites/carlieporterfield/2021/06/03/department-of-justice-creates-new-task-force-to-take-on-ransomware-attacks/ (accessed Aug. 27, 2021).
[19] “Reputational damage and cyber risk go hand in hand | Aon.” https://www.aon.com/unitedkingdom/insights/reputational-damage-and-cyber-risk.jsp (accessed Aug. 27, 2021).
[20] “How data breaches affect stock market share prices,” *Comparitech*, Nov. 06, 2019. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/ (accessed Aug. 27, 2021).
[21] N. Goud, “Kaspersky survey confirms 31 percent cyber attacks lead to job losses,” *Cybersecurity Insiders*, Sep. 14, 2018. https://www.cybersecurity-insiders.com/kaspersky-survey-confirms-31-percent-cyber-attacks-lead-to-job-losses/ (accessed Aug. 27, 2021).
[22] F. Imbert, “Capital One shares dive after data breach affecting 100 million,” *CNBC*, Jul. 30, 2019. https://www.cnbc.com/2019/07/30/capital-one-shares-dive-after-data-breach-affecting-100-million.html (accessed Sep. 03, 2021).
[23] D. Swinhoe, “Why businesses don’t report cybercrimes to law enforcement,” *CSO Online*, May 30, 2019. https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html (accessed Aug. 27, 2021).
[24] “SEC Brings Enforcement Action for Failure to Issue Timely Disclosure of Cyber Breach.” https://www.americanbar.org/groups/business_law/publications/blt/2018/06/cyber-breach/ (accessed Aug. 27, 2021).
[25] “Ransomware,” *Federal Bureau of Investigation*. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (accessed Aug. 27, 2021).
[26] “Many ransomware attacks go unreported. The FBI and Congress want to change that.,” *Washington Post*. Accessed: Aug. 27, 2021. [Online]. Available: https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/
[27] “80% of ransomware victims suffer repeat attacks, according to new report.” https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/ (accessed Aug. 27, 2021).
[28] J. Wolff, “How Quickly Should Companies Have to Disclose Data Breaches?,” *Slate Magazine*, Jun. 24, 2021. https://slate.com/technology/2021/06/data-breach-disclosure-law-warner-rubio-collins.html (accessed Aug. 27, 2021).
[29] nicole.keller@nist.gov, “Cybersecurity Framework,” *NIST*, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Feb. 11, 2021).
[30] “The 18 CIS Controls,” *CIS*. https://www.cisecurity.org/controls/cis-controls-list/ (accessed Aug. 27, 2021).
[31] M. Miller, “White House cyber chief backs new federal bureau to track threats,” *TheHill*, Aug. 02, 2021. https://thehill.com/policy/cybersecurity/566007-white-house-cyber-chief-backs-new-federal-bureau-to-track-cyber-threats (accessed Aug. 27, 2021).
[32] “MIT SCRAM – Secure Cyber Risk Aggregation and Measurement.” https://scram.mit.edu/ (accessed Aug. 27, 2021).
[33] “Sneak peek: V7.1 is a new way to look at the CIS Controls™,” *CIS*, Feb. 28, 2019. https://www.cisecurity.org/blog/sneak-peek-v7-1-new-way-to-look-at-cis-controls/ (accessed Aug. 27, 2021).
[34] “Biden to host tech, finance and energy CEOs for security summit at White House following

wave of cyberattacks," *CNBC*. https://www.cnbc.com/2021/08/25/biden-to-host-tech-finance-and-energy-ceos-for-white-house-cybersecurity-summit.html (accessed Aug. 27, 2021).
[35]"Biden tells top CEOs at White House summit to step up on cybersecurity," *Washington Post*. Accessed: Aug. 27, 2021. [Online]. Available: https://www.washingtonpost.com/technology/2021/08/25/white-house-cybersecurity-summit-apple-amazon/

Appendix A: Survey instrument / template

Status
Ready

Maturity levels

Category	Control	Not Implemented	Partially Implemented	Largely Implemented	Fully Implemented
1. MFA	1a. Deploy multi-factor authentication across the enterprise				
2. EDR	2a. Deploy an endpoint detection and response (EDR) system / host-based IPS agent				
	2b. Hunt for malicious activity				
3. Encryption	3a. Encrypt data in transit				
	3b. Encrypt data at rest				
4. Empowerment	4a. Remove barriers to sharing				
	4b. Receive external threat intelligence				
5. Training	5a. Evaluate skills				
	5b. Deliver regular training				
6. Backup	6a. Perform regular backups of systems				
	6b. Test backup data				
	6c. Protect backups				
	6d. Store backups in offline location				
7. Patch	7a. Deploy updates and patches in a timely manner				
	7b. Implement a centralized patch management system				
	7c. Apply patches using a risk-based approach				
8. Incident response	8a. Codify an incident response plan				
	8b. Test your incident response plan				
	8c. Maintain your incident response plan				
9. Check the work	9a. Establish an external penetration testing program				
	9b. Perform red team exercises				
10. Segment	10a. Adopt network segmentation to ensure isolation of critical systems in an attack				

Ransomware Incidents

11. Incidents	Indicate the total number of ransomware incidents against your organization within the past year (i.e., the last 12 months).	
12. Payments	Indicate the total number of ransomware payments made either directly or via a cybersecurity insurance company over the past year. This number should not be greater than the quantity in #11 above.	
13. Losses	Indicate the aggregate (sum total) US Dollar amount your organization paid out to ransomware attackers over the past year, either directly or via a cybersecurity insurance company.	
14. Resiliency	Incidate the estimated average number of hours it took to return to normal business operations across all ransomware incidents over the past year.	