RANSOMWARE TASK FORCE

Blueprint for Ransomware Defense

An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises

IST Institute for SECURITY + TECHNOLOGY

Primary Authors

Aaron McIntosh, Director - Product Marketing, ActZero

Valecia Stocchetti, Sr. Cybersecurity Engineer, CIS

Contributors

ActZero

Aaron McIntosh, Director - Product Marketing, ActZero

CYBER THREAT ALLIANCE

Michael Daniel, President, Cyber Threat Alliance

GLOBAL CYBER ALLIANCE

Brian Cute, Director, Capacity & Resilience Program, Global Cyber Alliance
Leslie Daigle, Chief Technical Officer and Internet Integrity Program Director, Global Cyber Alliance
Renee McLaughlin, Product Owner, Toolkits, Capacity & Resilience Program, Global Cyber Alliance

VENABLE LLP

John Banghart, Senior Director of Cybersecurity Services, Venable LLP

CIS Center for Internet Security®

Curt Dukes, Executive Vice President, Security Best Practices, CIS
Phyllis Lee, Sr. Director of Controls, CIS
Valecia Stocchetti, Sr. Cybersecurity Engineer, CIS
Brian de Vallance, Senior Advisor, CIS

IST Institute for SECURITY + TECHNOLOGY

Megan Stifel, Chief Strategy Officer, Institute for Security and Technology

resilience

Davis Hake, Co-Founder, Resilience

SecurityScorecard

Sachin Bansal, Chief Business and Legal Officer, SecurityScorecard
Charlie Moskowitz, Vice President, Policy & Government Affairs, SecurityScorecard

Endorsed by

INTERNATIONAL COUNTER RANSOMWARE INITIATIVE

This product does not reflect the views, laws, or practices of all members of the International Counter Ransomware Initiative (CRI). No member country is bound by the guidelines or recommendations set forth in this product.

Contents

Executive Summary

According to the U.S. Small Business Administration, there are 32,540,953 million small businesses in the United States, representing 99.9% of all firms.[1] However, many of these businesses remain inadequately prepared against the risk of a cyber attack. Accenture's 2019 Cost of Cybercrime Study, for example, revealed that "43% of cyber attacks target small businesses, but only 14% are prepared to defend themselves."[2] To address this risk, it is increasingly common for SMEs to obtain cybersecurity insurance. Increasingly, however, insurers require enterprises to better understand, implement, and demonstrate cyber risk management practices before qualifying.

It is in this context that we recommend that SMEs should adopt a cybersecurity framework of specific best practices to help defend against these attacks. Fortunately, adopting and following a security framework can help enterprises build stronger defenses. Unfortunately, it is difficult to know where to start, leaving many lost and unable to prioritize their cybersecurity efforts. However, that framework needs to be written in plain terms, with easily digestible and practical guidance. Regrettably, some SMEs believe they are unable to achieve and implement certain cybersecurity frameworks and therefore have not pursued business opportunities that require demonstration of compliance to them. This practice perpetuates the cycle of inefficient cybersecurity preparedness.

In response to Action 3.1.1 of the Ransomware Task Force (RTF) report, which calls for the cybersecurity community to "develop a clear, actionable framework for ransomware mitigation, response, and recovery," the Blueprint for Ransomware Defense Working Group developed a Blueprint comprised of a curated subset of essential cyber hygiene[3] Safeguards from the Center for Internet Security Critical Security Controls® (CIS Controls®) v8. These Safeguards represent a minimum standard of information security for all enterprises and are what should be applied to defend against the most common attacks. This Blueprint for Ransomware Defense represents a set of Foundational and Actionable Safeguards, aimed at small- and medium-sized enterprises[4] (SMEs).

Consequently, this Blueprint for Ransomware Defense utilizes the CIS Controls, a prioritized and prescriptive set of actions developed by a global community of cybersecurity experts. The forty (40) recommended Safeguards included in the Blueprint have been carefully selected not only for their ease-of-implementation but their effectiveness in defending against ransomware attacks. This has been backed by analysis from the CIS Community Defense Model v2.0 (CIS CDM v2.0), where implementing the Safeguards in this Blueprint defends against over 70%[5] of the attack techniques associated with ransomware. It is important to note that this Blueprint is not intended to serve as an implementation guide, but rather a recommendation of defensive actions that can be taken to protect against and respond to ransomware and other common cyber attacks. Appendix C of this document and this corresponding document provide several tools and resources that can be used to assist with implementation of these Safeguards.

Target Audience

The Working Group specifically created the Blueprint to remove a critical barrier for SMEs with limited cybersecurity expertise in defending against ransomware. It is written in plain terms, with descriptions of how the recommended Safeguards work to mitigate the associated risks. The Blueprint provides information that is useful to both business leaders and technical personnel, who need to work together to understand the risks and prioritize actions.

1 U.S. Small Business Advisory Office of Advocacy, SMB FAQs, December 2021, https://advocacy.sba.gov/wp-content/uploads/2021/12/Small-Business-FAQ-Revised-December-2021.pdf.

2 Accenture, Ninth Annual Cost of Cybersecurity, March 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.

3 Essential cyber hygiene consists of Safeguards from Implementation Group 1 (IG1) of the CIS Controls.

4 Enterprises include both businesses as well as government organizations.

5 As presented in the CIS Community Defense Model (CDM) v2.

Introduction

The RTF called for the cybersecurity community to "develop a clear, actionable framework for ransomware mitigation, response, and recovery." The basis for this Blueprint is the CIS Controls, a set of well-regarded and widely-used best practices that help enterprises focus their resources on the critical actions needed to defend against the most common cyber attacks. It includes a subset of these best practices, or “Safeguards,” that are most relevant to combating ransomware.[6]

CIS designed the selected Safeguards for SMEs that have small Information Technology (IT) teams with limited cybersecurity expertise and who typically defend against general, non-targeted attacks. These Safeguards provide "essential cyber hygiene," the protective controls and foundational capabilities necessary for implementing more advanced capabilities. Success is a direct result of planning and preparation. Just like a building or fire drill, the stronger the foundation and plan, the more likely the enterprise will be able to withstand a cybersecurity attack, that can happen quickly, unexpectedly, and bring an unprepared enterprise to an abrupt halt.

To help enterprises further prioritize their activities, this Blueprint divides the selected Safeguards into two types: Foundational and Actionable. The Foundational Safeguards are the set of practices an enterprise must implement in order to effectively undertake any other cybersecurity action. The Actionable Safeguards then build on the Foundational ones to increase an enterprise’s cybersecurity posture.

We encourage SMEs to implement as many of these Safeguards as possible, and we understand that not every enterprise can implement all Safeguards. While the Working Group recommends full implementation of the Blueprint’s Safeguards, any attempt at partial implementation of a Safeguard is an important step in increasing an enterprise’s cybersecurity. Perfection is not the goal. If the majority of SMEs implement these controls, our enterprise community will be more resilient and cyber-secure.

How to Use this Blueprint

Adopters should use this Blueprint as a starting point to prioritize their cybersecurity defenses. Appendix A includes a full list of Safeguards for ransomware defense. Several tools and resources, found in Appendix C and the Blueprint Tools and Resources, are available to assist with implementation of these Safeguards. Inclusion of tools within the accompanying document in no way represents or implies endorsement by the Blueprint for Ransomware Defense Working Group of any particular solution; nor does this inclusion of any tool or solution constitute a guarantee by the Blueprint for Ransomware Defense Working Group of the success of the tool or solution in providing cybersecurity coverage that shall improve ransomware protection.

Acknowledgement of Risk

This Blueprint places a heavy emphasis on implementing protective measures and building the capacity to implement more advanced capabilities. While analysis indicates that essential cyber hygiene defends against over 70%[7] of the attack techniques associated with ransomware, how well they are implemented and how determined adversaries are will determine their ultimate effectiveness.

As will be conveyed below, essential cyber hygiene represents a minimum standard of information security for all enterprises and are the on-ramp to implementing additional CIS Controls. This Blueprint is what every enterprise should apply to defend against the most common attacks. SMEs may find it necessary to implement additional Safeguards in order to defend against more advanced attacks.

6 These practices are drawn from CIS Controls v8 Implementation Group 1 (IG1).

7 As presented in the CIS Community Defense Model (CDM) v2.0.

Blueprint for Action

In order to defend against ransomware, SMEs must implement a layered approach to protect their most critical assets. This requires implementation of controls in areas such as enterprise asset and software inventory management, vulnerability management, malware defense, training, data recovery, and incident response. As ransomware evolves, adversaries are now crafting new techniques, such as extortion – where attackers exfiltrate data prior to encryption and then demand payment to avoid public release of the data. By implementing the Safeguards in this Blueprint, SMEs are well-poised to defend against ransomware, as well as other types of attacks.

The following describes Foundational and Actionable Safeguards for ransomware defense and why they are important. **Users of this Blueprint should focus on implementing Foundational Safeguards first before implementing Actionable (i.e., more technical) Safeguards.**

Alignment to the NIST Cybersecurity Framework Functions

Given its broad acceptance across the government, business, and cybersecurity communities, the Blueprint for Ransomware Defense Working Group aligned the subset of Safeguards to the National Institute of Standards and Technology® Cybersecurity Framework (NIST® CSF) functions – Identify, Protect, Detect, Respond, and Recover – that help implement an effective cybersecurity program. Grouping actions by these functions can help SMEs better understand their risks, the steps needed to protect their enterprise from that risk, the tools that can be used to find and detect risks, and the solutions available to contain and remediate threats as quickly as possible.

Due to their complexity and technical nature, Safeguards relating to the "Detect" function have been excluded from this Blueprint. However, the Working Group strongly recommends that SMEs following this Blueprint work with a cybersecurity services provider to implement detection controls, or other controls where SMEs require assistance, where appropriate.

Overview of the Safeguards

The Blueprint includes a total of 40 Safeguards, including 14 Foundational and 26 Actionable Safeguards. The Blueprint first groups these actions by the NIST CSF functions. Within each function, the Blueprint presents the Safeguards in priority order based on their value in combating ransomware and to a general cybersecurity defense posture.[8]

FOUNDATIONAL SAFEGUARDS

Foundational Safeguards are the building blocks that are necessary to establish an enterprise's cyber security program. They also enable the implementation of Actionable Safeguards. Fourteen (14) Foundational Safeguards were selected and prioritized within the Blueprint, as described below.

Identify

In order to defend your network, you must first know what is on your network, meaning what technology you are using and data you are storing and/or transmitting. Foundational Safeguards under Identify recommend that SMEs establish and maintain enterprise asset and software inventories to better manage all connected devices; and implement data management processes that clearly outline the collection, use, and storage of data. Activities also include establishing and maintaining an inventory of accounts, including regular user accounts and those with elevated privileges.

These Safeguards are imperative to protecting against and responding to a ransomware incident. Without knowing the assets, software, and accounts on an enterprise's network, it becomes difficult to defend against

8 The Working Group used the analysis of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Framework conducted by CIS and presented in their CIS Community Defense Model (CDM) v2.0 to derive the prioritization.

and respond to an incident. For example, unknown devices may be more easily compromised and used by an attacker within your environment. This could increase the risk to the enterprise and could result in additional attacks or prolong the same attack. Knowing your environment sets the stage for implementing essential cyber hygiene on all your devices.

Safeguards:

- Establish and Maintain Detailed Enterprise Asset Inventory
- Establish and Maintain a Software Inventory
- Establish and Maintain a Data Management Process
- Establish and Maintain an Inventory of Accounts

While these Safeguards are very complex to manage, as new assets are always being added to the network, they are foundational for effective defense and play a critical role in other defensive activities, such as backups and incident response. Additionally, data is no longer contained only within the four walls of an enterprise. Mobile and portable devices connect back to enterprise resources, making it challenging to manage the data without proper Safeguards in place.

Protect

Once a SME knows what is on their network, the next step is to implement Safeguards to protect those assets, data, and users from malicious actors looking to harm them.

Secure Configurations

Configuration management processes are important for implementing and maintaining security over time. These Safeguards focus on how devices and the overall network are laid out and the rules by which those devices and the network operate, collectively referred to as a "configuration." These configuration Safeguards include the implementation of secure configuration processes for enterprise assets, such as laptops, desktops, servers, and mobile devices, to name a few. A process for configuring network infrastructure is also important, including devices such as firewalls, routers, and switches. The addition of enterprise assets, software, users, etc. can add risk if strong processes are not in place to ensure the (re-)application of appropriate security controls. For example, a software update may change a configuration setting and make it less secure. An enterprise should have a secure configuration process in place that addresses security "drift" over time by checking for whether assets comply with established configurations and policies, and, if not, putting those assets back into compliance.

Account and Access Management

User accounts may have a wide variety of access to basic functions such as email, to higher privileged accounts that can access nearly everything in the enterprise. The Foundational Safeguards in Protect require an enterprise to establish a process for granting and revoking permissions to enterprise systems. Ensuring that an enterprise follows the principle of least privilege – users should only be given privileges that they need to complete a task – is also critical. This includes when personnel change roles or require new (or temporary) permissions for a project as well as when personnel join and leave the enterprise.

Vulnerability Management Planning

Security researchers and other stakeholders find and publish over 18,000 software vulnerabilities each year, and while there are always more that are unknown to the broader community, malicious actors typically use known vulnerabilities first. Thus, vulnerability management plays a critical role in protecting an enterprise's infrastructure. The Blueprint recommends two Safeguards for implementing vulnerability management and risk remediation processes. These Safeguards encompass applying operating system and application patches

in a timely manner. This process applies not only to assets and software but also network devices that are used to manage and/or monitor those assets and software.

Security Awareness & Skills Training

While investments in technology are important, people are an essential resource in building up good defenses against ransomware and other attacks. According to the recent 2021 Verizon Data Breach Investigations Report (DBIR)[9], 85% of breaches involved a human-element. This Blueprint calls for SMEs to establish and maintain a security awareness program for all employees, partners, and third-party users. This not only involves training personnel on how to interact with enterprise networks and systems securely, but also ensuring that personnel understand why it is important and the role they have in protecting the enterprise.

Safeguards:

- Establish and Maintain a Secure Configuration Process
- Establish and Maintain a Secure Configuration Process for Network Infrastructure
- Establish an Access Granting Process
- Establish an Access Revoking Process
- Establish and Maintain a Vulnerability Management Process
- Establish and Maintain a Remediation Process
- Establish and Maintain a Security Awareness Program

Respond

Preparation is key with incident response. Having a plan before an incident occurs ensures that the enterprise knows what to do when an attack occurs. The Safeguards in Respond help reduce operational downtime when controls may fail and an attacker has been successful in causing harm.

Under these Safeguards, enterprises establish incident reporting and security log management processes. At a minimum, SMEs should have a process for personnel to report security incidents. This process should include establishing a reporting timeframe, who to report it to, how to report it, and the information needed for the report. Having recovery measures in place enables enterprises to become fully operational in quick order minimizing downtime, loss of revenue, and brand damage. Enterprises should run regular, impromptu fire drills on the Incident Response (IR) plan to set the stage for the best outcomes in a real event.

Logging is also critical for an enterprise to successfully respond to an incident. The first step to log management is to establish a process. This ensures that the enterprise knows which logs should be collected at a minimum, how often they should be reviewed, and how long they should be retained. Should an enterprise become compromised, logs will be needed for incident response to help determine the source of an attack or provide evidence for legal purposes.

Safeguards:

- Establish and Maintain an Enterprise Process for Reporting Incidents
- Establish and Maintain an Audit Log Management Process

Recover

One of the most significant harms caused by ransomware is a loss of data that is essential for the SME to operate. The Blueprint includes a Foundational Safeguard requiring SMEs to establish and maintain a data recovery process as part of response and recovery planning. New techniques in ransomware (e.g., extortion)

9 *2021 Verizon Data Breach Investigations Report* (DBIR) https://verizon.com/dbir.

pose challenges to enterprises who have good data recovery controls but poor data protection controls, which is why successful recovery from a ransomware incident requires both.

Safeguards:

- Establish and Maintain a Data Recovery Process

ACTIONABLE SAFEGUARDS

In addition to the Foundational Safeguards, long-term, effective security requires taking additional actions. The Blueprint's twenty-six (26) selected and prioritized Actionable Safeguards enables an enterprise to improve its security and defend against ransomware and other general, non-targeted cyber attacks. The Actionable Safeguards build on the Foundational ones and are all about applying the technical controls needed to protect an enterprise's environment.

Identify

Following on from the Foundational Identify Safeguards that established knowledge about the devices and data in the SMEs environment, the Blueprint's Actionable Safeguard within the Identify category requires SMEs to ensure that they are always using authorized and the most up-to-date software available across their enterprise assets. Adversaries continuously scan networks to exploit vulnerable versions of software. Software vulnerabilities remain one of the top initial attack vectors for ransomware attacks so keeping software up to date and auditing that list of software frequently will help to reduce the risk of exploitation.

Safeguard:

» Ensure Authorized Software is Currently Supported

Protect

Nearly 70% of the Blueprint's Actionable Safeguards fall into the Protect function. The Protect function is essential because its purpose is to focus on limiting or containing the impact of a potential cybersecurity event. The recommended Safeguards include both technical and training Safeguards. Technical Safeguards include implementing and managing firewalls on company servers, managing removable media security, as well as deploying and managing anti-malware software, just to name a few. Training Safeguards address educating personnel on how to recognize an attack and how to report it.

Secure Configurations

While ransomware has a variety of initial infection vectors, three vectors constitute the bulk of intrusion attempts: use of the Remote Desktop Protocol (RDP) – a protocol used to remotely manage Windows devices, phishing (typically malicious emails that appear to come from reputable sources but aim to steal credentials or sensitive information), and exploitation of software vulnerabilities. Hardening assets, software, and network devices defends against these top attack vectors and closes security gaps that may linger from insecure default configurations. Failure to disable/remove default accounts, change default passwords, and/or alter other vulnerable settings increases the risk of exploitation by an adversary. Safeguards in this section call for SMEs to implement and manage a firewall on servers and manage default accounts on enterprise networks and systems.

Following best practice guidance (e.g., CIS Benchmarks™, Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)) is also recommended when securely configuring systems.

Account and Access Management

Once an attacker obtains credentials to an account, especially accounts with elevated privileges, the potential harm they can cause increases significantly. Not only may they be able to enter an enterprise's network, but they may also be able to move within the network to compromise neighboring accounts and systems. The Blueprint recommends several activities to reduce the risk for an account compromise, to include regular assessments of privileged access rights, removal of dormant accounts, proper password management to avoid the trap of password reuse, and implementation of multi-factor authentication (MFA) across enterprise systems. Enabling

MFA is especially important as it creates an added layer of security if a password is compromised. Account and access management also applies to cloud-based platforms, especially cloud-based email services that may connect to other enterprise resources.

Vulnerability Management Planning

Ransomware continues to prey on enterprises who fail to implement patches for known vulnerabilities in a timely manner. Several public reports highlight that attackers are not only exploiting recently revealed vulnerabilities but ones that are several years old. Several vulnerability management Safeguards are recommended in the Blueprint, including improving patch management and ensuring networks and devices are running the latest system updates. Vulnerability management is especially important on legacy systems that may be running outdated software that the vendor no longer supports, leaving the system vulnerable to an attack. If a legacy system is unable to be updated, alternative controls for these systems must be implemented to ensure that they are adequately protected, or a replacement solution should be implemented.

Enterprises should consider automating patching for operating systems such as Microsoft® Windows® and Apple® macOS®. If patching is not automated, enterprises, or their security partners, must pay particular attention to critical or zero-day vulnerabilities announced in the security notification and updates from each vendor, and expeditiously implement patch guidance.

Malware Defenses

Ransomware can be delivered in several ways, including through emails (via a link or attachment), web browsers, and removable media. A number of Safeguards in the Blueprint relate to malware defenses including the deployment of anti-malware tools to prevent attacks from executing on enterprise assets, as well as keeping the anti-malware software and signatures up to date. Keeping browsers and email clients up to date is also important to prevent exploits from happening through these applications. Removable media (e.g., USBs) poses a risk as well. Features such as autorun and autoplay can enable content to automatically execute on a system when removable media is connected or plugged in. If a removable media device is infected with malware and gets inserted into the system, it can infect the targeted system and neighboring systems. Disabling these features reduces the risk.

Another popular vector for ransomware is through malicious URLs (Uniform Resource Locators). This can be delivered via email or directly through a web browser. Wherever it might originate, controls, such as DNS (Domain Name System) filtering, can prevent malware from being downloaded to a victim's system or prevent a user from seeing a phishing page (therefore preventing credentials from being sent to an attacker or a malicious file being downloaded). Many DNS filtering services are available for free and are a quick and easy way to mitigate an enterprise's risk.

Security Awareness & Skills Training

Addressing internal gaps, such as lack of training, is critically important. With the continued growth of phishing and smishing attacks (text messages tricking users to divulge sensitive information or download malicious applications), the Blueprint recommends that SMEs train their workforce to recognize social engineering attacks and to recognize and report security incidents.

Training personnel on how to recognize a social engineering attack is critical to establishing defenses in a network. While tools and technology can be put in place to defend against phishing, they are not 100% effective, leaving the enterprise's personnel to be the main line of defense.

Equally important is training personnel on how to report a security incident. With any type of attack, timing is of the essence. Quick reporting followed by quick action can interrupt an attack, stopping or reducing harm. Training is essential to ensure personnel understand what to do and how to do it.

Safeguards:

» Manage Default Accounts on Enterprise Assets and Software

» Use Unique Passwords

- Disable Dormant Accounts
- Restrict Administrator Privileges to Dedicated Administrator Accounts
- Require MFA for Externally-Exposed Applications
- Require MFA for Remote Network Access
- Require MFA for Administrative Access
- Perform Automated Operating System Patch Management
- Perform Automated Application Patch Management
- Ensure Use of Only Fully Supported Browsers and Email Clients
- Use DNS Filtering Services
- Ensure Network Infrastructure is Up-to-Date
- Deploy and Maintain Anti-Malware Software
- Configure Automatic Anti-Malware Signature Updates
- Disable Autorun and Autoplay for Removable Media
- Train Workforce Members to Recognize Social Engineering Attacks
- Train Workforce Members on Recognizing and Reporting Security Incidents

Respond

The unfortunate reality is that, sometimes even the best protections cannot stop a dedicated adversary willing to invest the time and effort needed to disrupt an enterprise. Actionable Safeguards in the Respond function include reporting incidents, establishing key contacts, how and when to engage them, and the process and tools required for adequate log collection and storage.

Having at least one person who will manage the incident handling process will help with coordination efforts during incident response. This may include internal employees or third-party vendors, or a combination of both. Creating a list of contacts to inform them of the incident is also helpful to prepare an enterprise beforehand. Contacts may include internal staff, law enforcement, insurance providers, government agencies, legal counsel, or other stakeholders. Communication is key during an incident as there are a lot of moving parts.

The collection of audit logs prior to an incident is also important. This may include logs from operating systems, applications, or network devices. During an incident, logs can be extremely useful to analyze and can help to piece together what happened. More importantly, this analysis can be used to apply mitigations to prevent the attack from happening again. Ensuring there is adequate log storage is also important, as log files can quickly take up space on a system, impacting the performance of a system.

Safeguards:

- Designate Personnel to Manage Incident Handling
- Establish and Maintain Contact Information for Reporting Security Incidents
- Collect Audit Logs
- Ensure Adequate Audit Log Storage

Recover

Having good backups of essential data is one of the most effective strategies to recover from a ransomware attack. The Blueprint prescribes a number of Actionable Safeguards for data recovery including measures for both establishing and restoring data back-ups. Automating the backup process, protecting that data, and ensuring that it is not regularly connected to the network are all important when it comes to recovering from a ransomware attack. The last piece is important because you can implement all the right controls to protect

the backup data, but if it is stored directly on the system or network that is being ransomed then that data also becomes encrypted.

Safeguards:

- Perform Automated Backups
- Protect Recovery Data
- Establish and Maintain an Isolated Instance of Recovery Data

Using the Blueprint to Strengthen Cyber Insurance

The RTF estimates that in 2021, victims paid $602 million in ransomware extortions, a 70% increase since 2020. Ransomware incidents accounted for 79% of business interruption claims driving policy premiums up at greater than 90% year-over-year. This is untenable for insureds and the market and is part of the reason many cyber insurance providers have been eager to support the work of the RTF.

Starting as a new coverage two decades ago for corporate data breach liability, cyber insurance has evolved dramatically in the past decade into a critical tool for managing corporate cybersecurity risk. Within the Blueprint we discuss Safeguards that are categorized as Foundational or Actionable. SMEs can look to their cyber insurers for help and guidance with implementing many of these controls. Most cyber insurers have proactive offerings at reduced rates available that will significantly reduce the cost and complexity of implementing many of the Safeguards in this Blueprint. However, the explosion in the effectiveness and scale of ransomware attacks has been a significant challenge to the market that insurers and others use to measure legal liability from large data breach events.

The Blueprint for Ransomware Defense provides two critical elements for the cyber insurance industry's fight against the rise in criminal ransomware attacks.

- First, the Blueprint provides a practical, data driven, guide specifically for middle market and small business companies that often struggle the most with defending their systems. Starting with the CIS Critical Security Controls Implementation Group 1 (IG1) Safeguards, the Working Group down selected these security measures to the top most critical defenses against ransomware. They have also been reviewed by insurance professionals to ensure they match with what is actively being seen in insurance claims and could help lower the likelihood of attacks.
- Second, the Blueprint helps the insurance industry better understand what signals to look for when underwriting accounts. In other lines of insurance, engineering-based loss data drives underwriting and risk mitigation efforts by carriers and reinsurers. Because of its human adversarial element and highly technical nature, cyber insurance has often relied on data breach litigation data to drive actuarial pricing and determine underwriting guidelines. The rise in ransomware has dramatically shown the need for a greater focus on security controls that can both stop attacks and speed recovery so that those insured are not forced to pay an extortion to quickly recover their critical systems.

Consistent with many of the Blueprint's recommendations, some of the specific security controls that the cyber insurance industry has seen lower incident costs and actively looks at during the underwriting process include:

- Implementation of strong backups;
- Security awareness and incident response training;
- Email security deployed across the entire enterprise;
- Advanced endpoint protection against malware; and
- Network visibility and security.

We have also included several incident response resources in the Blueprint Tools and Resources so that enterprises without fully developed security policies can have an industry developed starting point for bringing cybersecurity to an executive level in their enterprise.

Conclusion

The forty (40) recommended Safeguards included in the Blueprint have been carefully selected not only for their ease-of-implementation but their effectiveness in defending against ransomware attacks. Essential cyber hygiene is intended to empower SMEs to mitigate, respond, and recover from a ransomware event. Implementing as many of these Safeguards as possible should be part of an iterative risk management program at every enterprise. SMEs who implement essential cyber hygiene will achieve a high level of protection and be well-positioned to defend against ransomware. They will also be able to manage their cyber risk more effectively and have the capacity to implement additional controls as needed to address specific threats.

Finally, the Blueprint for Ransomware Defense Working Group seeks to remove barriers to adoption wherever possible, and to that end, we have included tools and resources that can be used to implement each of the Safeguards. Where those resources seem lacking, ask questions and seek guidance from cybersecurity providers. While perfect cybersecurity is impossible, you can make your company more resistant and resilient to cyber threats.

How to Get Started

As mentioned previously, many SMEs can become overwhelmed when implementing a security framework. It is important to start small and grow your defenses at a pace that is appropriate for your enterprise. To begin, enterprises should download the Blueprint Tools and Resources to assess which Safeguards are recommended for implementation. This document provides the Safeguard's description, associated NIST CSF functions, as well as several tools and resources that can be used to assist with implementation.

Additionally, there are many other tools and resources that can help with an enterprise's journey towards essential cyber hygiene. For example, some enterprises may already be implementing another security framework and may be hesitant to move to or introduce another security framework into their enterprise. Fortunately, CIS maps to several other security frameworks (e.g., NIST, Cybersecurity Maturity Model Certification (CMMC)) and makes those mappings freely available via the CIS Controls Navigator and CIS WorkBench for all enterprises to use. For enterprises who want to learn more about the CIS Controls specifically and how to get started with implementing this Blueprint, there are several resources that can be used including:

- CIS Controls Assessment Specification – Provides an understanding of what should be measured in order to verify that CIS Safeguards are properly implemented.
- CIS Controls Self Assessment Tool (CIS CSAT) – Tool to assess and track implementation of the CIS Controls.
- CIS Risk Assessment Method (CIS RAM) v2.1 – An information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls.

Several other reputable resources can also be found in Appendix C of this document. As previously mentioned, 100% perfection is not the goal. Any step forward is a path towards establishing essential cyber hygiene. Defending against ransomware and cyber threats in general is no small task, but one that is very much needed in order to strengthen the cybersecurity posture of enterprises across the globe. Our Working Group is confident that the Safeguards selected will help to defend against ransomware and other cyber attacks as well as help build a strong foundation for effective cyber defense.

Appendix A: Blueprint for Ransomware Defense

Category	CIS Safeguard #	NIST Security Function	CIS Safeguard Title	Type
Identify				
Know Your Environment	1.1	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Foundational
	2.1	Identify	Establish and Maintain a Software Inventory	Foundational
	2.2	Identify	Ensure Authorized Software is Currently Supported	Actionable
	3.1	Identify	Establish and Maintain a Data Management Process	Foundational
	5.1	Identify	Establish and Maintain an Inventory of Accounts	Foundational
Protect				
Secure Configurations	4.1	Protect	Establish and Maintain a Secure Configuration Process	Foundational
	4.2	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Foundational
	4.4	Protect	Implement and Manage a Firewall on Servers	Actionable
	4.7	Protect	Manage Default Accounts on Enterprise Assets and Software	Actionable
Account and Access Management	5.2	Protect	Use Unique Passwords	Actionable
	5.3	Protect	Disable Dormant Accounts	Actionable
	5.4	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Actionable
	6.1	Protect	Establish an Access Granting Process	Foundational
	6.2	Protect	Establish an Access Revoking Process	Foundational
	6.3	Protect	Require MFA for Externally-Exposed Applications	Actionable
	6.4	Protect	Require MFA for Remote Network Access	Actionable
	6.5	Protect	Require MFA for Administrative Access	Actionable
Vulnerability Management Planning	7.1	Protect	Establish and Maintain a Vulnerability Management Process	Foundational
	7.2	Protect	Establish and Maintain a Remediation Process	Foundational
	7.3	Protect	Perform Automated Operating System Patch Management	Actionable
	7.4	Protect	Perform Automated Application Patch Management	Actionable
	12.1	Protect	Ensure Network Infrastructure is Up-to-Date	Actionable
Malware Defense	9.1	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Actionable
	9.2	Protect	Use DNS Filtering Services	Actionable
	10.1	Protect	Deploy and Maintain Anti-Malware Software	Actionable
	10.2	Protect	Configure Automatic Anti-Malware Signature Updates	Actionable
	10.3	Protect	Disable Autorun and Autoplay for Removable Media	Actionable
Security Awareness & Skills Training	14.1	Protect	Establish and Maintain a Security Awareness Program	Foundational
	14.2	Protect	Train Workforce Members to Recognize Social Engineering Attacks	Actionable
	14.6	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	Actionable
Detect				
Respond				
Data Recovery & Incident Response	17.1	Respond	Designate Personnel to Manage Incident Handling	Actionable
	17.2	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	Actionable
	17.3	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Foundational
	8.1	Respond	Establish and Maintain an Audit Log Management Process	Foundational
	8.2	Respond	Collect Audit Logs	Actionable
	8.3	Respond	Ensure Adequate Audit Log Storage	Actionable
Recover				
Data Recovery & Incident Response	11.1	Recover	Establish and Maintain a Data Recovery Process	Foundational
	11.2	Recover	Perform Automated Backups	Actionable
	11.3	Recover	Protect Recovery Data	Actionable
	11.4	Recover	Establish and Maintain an Isolated Instance of Recovery Data	Actionable

Appendix B: Abbreviations and Acronyms

CIS	Center for Internet Security
CIS CDM	Center for Internet Security Community Defense Model
CIS Controls	Center for Internet Security Controls
CIS CSAT	Center for Internet Security ControlsSelf Assessment Tool
CIS RAM	Center for Internet Security Risk Assessment Method
CISA	Cyber and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CSF	Cybersecurity Framework
DISA STIGs	Defense Information Systems Agency Security Technical Implementation Guides
DNS	Domain Name System
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
GCA	Global Cyber Alliance
IG	Implementation Group
IG1	Implementation Group 1
IR	Incident Response
IT	Information Technology
ISO	International Organization for Standardization
IST	Institute for Security and Technology
MFA	Multi-factor authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
RDP	Remote Desktop Protocol
RTF	Ransomware Task Force
SMEs	Small- and medium-sized Enterprises
SLTT	State, Local, Tribal, and Territorial governments
USB	Universal Serial Bus

Appendix C: Links and Resources

Center for Internet Security Controls (CIS Controls) v8 – Learn more about the CIS Controls, including how to get started, why each Control is critical, procedures and tools to use during implementation, and a complete listing of Safeguards for each Control.

CIS Controls Assessment Specification – Provides an understanding of what should be measured in order to verify that CIS Safeguards are properly implemented.

CIS Controls Navigator – Learn how the Controls and Safeguards map to other security standards (e.g., CMMC, NIST SP 800-53 Rev. 5, MITRE ATT&CK).

CIS Controls Self Assessment Tool (CIS CSAT) – Tool to assess and track implementation of the CIS Controls.

CIS Community Defense Model (CDM) v2.0 – A guide published by CIS that leverages the open availability of comprehensive summaries of attacks and security incidents, and the industry-endorsed ecosystem – MITRE ATT&CK.

CIS Risk Assessment Method (CIS RAM) v2.1 – An information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls.

CIS SecureSuite Membership – Access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more. No-cost membership for State, Local, Tribal, and Territorial governments.

CIS Benchmarks™ – Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices.

Cybersecurity and Infrastructure Security Agency (CISA) & Multi-State Information Sharing and Analysis Center (MS-ISAC®) Joint Ransomware Guide – Ransomware best practices and recommendations are based on operational insight from CISA and the MS-ISAC®.

CISA | Stop Ransomware – The U.S. government's one-stop location to stop ransomware.

Cyber Readiness Institute | Ransomware Playbook – How to prepare for, respond to, and recover from a ransomware attack.

Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGS) – Configuration standards developed by the Defense Information Systems Agency.

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC®) Membership – Free for all SLTT government organizations that support the elections officials of the U.S., and associations thereof.

Federal Bureau of Investigation (FBI) | Ransomware Fact Sheet – Learn more about what ransomware is and what to do about it.

Global Cyber Alliance (GCA) | Cybersecurity Toolkit for Small Business – Free and effective tools you can use today to take immediate action to reduce your cyber risk.

Institute for Security and Technology (IST) | RTF Report: Combating Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force.

MS-ISAC Membership – Free for all 50 states, the District of Columbia, U.S. territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the U.S.

National Institute of Standards and Technology (NIST) – NIST Cybersecurity Framework

NIST Small Business Cybersecurity Corner – Ransomware resource page

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org