Getting Started with Cybersecurity Risk Management | Ransomware

Quick Start Guide

With the threat of ransomware growing, this "quick start guide" will help organizations use the National Institute of Standards and Technology (NIST) *Ransomware Risk Management: A Cybersecurity Framework Profile* to combat ransomware. Like the broader NIST Cybersecurity Framework, which is widely used voluntary guidance to help organizations better manage and reduce cybersecurity risk, the customized ransomware profile fosters communications and risk-based actions among internal and external stakeholders, including partners and suppliers.

The Framework is organized by five key Functions – Identify, Protect, Detect, Respond, and Recover. These five terms provide a comprehensive way to view the lifecycle for managing cybersecurity risk. The activities listed under each Function offer a good starting point for any organization, including those with limited resources to address cybersecurity challenges. They help to set priorities so that an organization gets the greatest value out of its efforts to manage ransomware risks. Much depends on how sophisticated your current operations are in terms of cybersecurity risk management. While there are many other things that can and should be done to combat ransomware, it is important to recognize that you don't need to do everything all at once. *Getting started is the key in cybersecurity, including managing ransomware risks!* NIST recommends taking these steps to help thwart ransomware...

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

- **Maintain hardware and software inventories.** It's important to understand what computer hardware and software is used by your enterprise. These are frequently the entry points of malicious actors who engage in ransomware attacks. This information helps remediate vulnerabilities that could be exploited in ransomware attacks and is also very useful in recovery. An inventory can be as simple as a spreadsheet. Software inventories should track software name and version, devices where it is currently installed, the last patch date, and known vulnerabilities.

- **Document information flows.** Knowing what type of information your enterprise collects and uses is vital, but so is understanding where data is located and flows, especially when contracts and external partners are engaged. Construct a record of information flows (e.g., connections among devices/internet protocol addresses) to help enumerate what information or processes are at risk if the attackers move laterally within an environment.

- **Identify the external information systems to which your enterprise connects.** In case of a ransomware event, you need to plan how you will communicate with partners and identify possible actions to temporarily disconnect from external systems. Identifying these connections will also help put security controls in place (e.g., access rights) and indicate areas where controls may be shared with third parties.

- **Identify critical enterprise processes and assets.** What are your enterprise's activities that absolutely must continue in order to be viable? This could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring the data your enterprise collects remains accessible and accurate. This information is essential to understanding the true scope and impact of ransomware events – and is vital in contingency planning for future ransomware events, emergency response, and recovery actions. Having this information in advance allows enterprises to prioritize resources. If you rely on an industrial control system (ICS), include its critical functions.

- **Establish cybersecurity policies that spell out roles and responsibilities.** These should clearly describe expectations for how your enterprise's cybersecurity activities – including actions by employees, contractors, and partners – will protect your information and systems and support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).

Last Updated: February 2022

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

PROTECT

Develop and implement the appropriate safeguards to ensure delivery of services.

➔ **Manage access to assets and information.** If you do nothing else, limit access to physical and computer-related assets and associated facilities to authorized users, processes, and devices – and manage access consistent with the risk to critical activities and transactions.

Start by creating unique accounts for each employee and ensure that users have access only to information, computers, and applications needed for their jobs. Choose standard user accounts versus accounts with administrative privileges wherever possible. Authenticate users by strong passwords or multi-factor techniques before they are granted that access.

Since most ransomware attacks are conducted remotely, controlling remote access is vital to maintaining the integrity of systems and data files to protect against malicious code insertion and data exfiltration. Restrict access to official networks from personal devices. Tightly manage and track physical access to devices, whether it is a laptop computer or a critical component of an industrial control system (ICS).

In larger or more complex organizations, network segmentation or segregation can limit the scope of ransomware events by preventing malware from proliferating among potential target systems. This is particularly important for critical ICS functions, including Safety Instrument Systems (SIS).

➔ **Manage device vulnerabilities.** Regularly update the operating system and the applications on your computers and other devices to protect them from attack. *Keep them fully patched!* If possible, enable automatic updates. Block access to ransomware sites. Consider using software tools to scan devices for additional vulnerabilities and remediate vulnerabilities with high likelihood or impact. Properly configuring change and update processes can help to discourage replacement of code with products that contain malware or do not satisfy access management policies.

➔ **Educate and train employees and other users.** Regularly train and retrain all users to be sure that they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities – and make it a condition of employment. Training those responsible for hardware and software installation, configuration, and maintenance is key, but equally important is training *all users* to always use antivirus software, to install only if they are approved by the organization, click only on verified links, to connect only to secured networks, and not to connect devices to public charging stations. Users should know that their access to official networks from personal devices is restricted. Most ransomware attacks are made possible by users who engage in unsafe practices, administrators who implement insecure configurations, or developers who have insufficient security training.

➔ **Protect your devices – securely.** Consider installing host-based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and a way to dispose of devices properly. These measures protect against installing ransomware and they also protect against data leaks.

➔ **Protect sensitive data.** Your organization likely stores or transmits sensitive data, so you should manage your information and records (data) consistent with your risk strategy to protect the confidentiality, integrity, and availability of information. Use integrity checking mechanisms (like digital signatures) to verify software, firmware, and information integrity and detect tampered software updates that can be used to insert malware.

➔ **Conduct regular backups.** Ensuring availability of data can reduce ransomware impacts. This includes the ability to maintain offsite and offline data backups, as well as testing the mean time to recovery and system redundancy. Many operating systems have built-in backup capabilities; software and cloud solutions are also available to automate backups. It's good practice to keep one frequently backed up set of data offline. Regular backups that are maintained and tested are essential to timely and relatively painless recovery from ransomware events. Secure backups and keep them offline so they cannot become corrupted or be deleted by ransomware or by an attacker.

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

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

- **Test and update detection processes.** Develop and test processes and procedures for detecting anomalous events such as unauthorized entities and actions on the networks and in the physical environment, including personnel activity. This includes determining the impact of events that can inform response and recovery priorities for a ransomware attack.

  Larger or more complex organizations should acquire and install Security Information and Event Management (SIEM) solutions that include multiple sources and sensors to improve network visibility, assist in the early detection of ransomware, and aid in understanding how ransomware may propagate through a network. These tools need to generate and record (log) activity. Logs are crucial to identifying anomalies in computers and applications; they record events such as changes to systems or accounts as well as communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.

- **Train staff.** Staff should be aware of their roles and responsibilities to detect and report within your organization and to external authorities. That requires training and retraining.

- **Know expected data flows.** If you know what and how data is expected to flow for your enterprise, you are much more likely to notice when the unexpected happens – and unexpected is never a good thing when it comes to cybersecurity. Unexpected data flows might include customer information being exported from an internal database and exiting the network. If you have contracted work to a cloud or managed service provider, discuss with them how they track data flows and report, including unexpected events.

- **Quickly communicate and determine the impact of cybersecurity events.** Timely communication of anomalous events is essential to taking remedial actions before a ransomware attack can be fully damaging. If a cybersecurity event is detected, your enterprise should work quickly and thoroughly to understand the breadth and depth of the impact. Seek help. Communicating with appropriate stakeholders and with law enforcement (e.g., FBI) will help keep you in good stead with partners, oversight bodies, and others (potentially including investors) and improve policies and processes.

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- **Develop response plans.** Like many other things, ransomware response starts with planning, including coordinating plans with internal and external stakeholders. Focus on procedures for immediate mitigation and containing the ransomware event and determining its impact.

- **Coordinate with internal and external stakeholders.** Include all key stakeholders and external service providers. Maintain a handy, up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources. Priorities include preemptive messaging and agreement on how to stem the spread of misinformation. Stakeholders can contribute to improvements in planning and execution.

- **Test response plans.** Testing helps to make sure each person knows their responsibilities in executing the plan. The better prepared your organization is, the more effective the response is likely to be. This includes knowing any legal reporting requirements or required information sharing.

- **Update response plans.** Testing the plan (and executing it during an incident) inevitably will reveal needed improvements. Be sure to update response plans with lessons learned. This will minimize the probability of future successful ransomware attacks and help to restore confidence among stakeholders.

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

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

- **Make contingency plans.** Like response, recovery from ransomware events begins well before an event with contingency planning. In this case, your enterprise should plan for restoration of systems capabilities and correction of vulnerabilities. Focus on procedures for immediate mitigation of the ransomware event, determining the event's impact, and notifying stakeholders.
- **Communicate with internal and external stakeholders.** Recovery depends upon effective communication. Your recovery plans need to carefully account for what, how, and when ransomware event information will be shared with various stakeholders so that all interested parties receive the information that they need, but no inappropriate information is shared.
- **Manage public relations and company reputation.** When developing a ransomware recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – and not reactionary.
- **Test and update recovery plans.** Testing the execution of recovery plans will improve employee and partner awareness and highlight areas for improvement. Always update plans with lessons learned.

WHERE TO FIND MORE NIST RANSOMWARE RESOURCES…

- ✓ **PROTECTION & RESPONSE RESOURCES:** https://csrc.nist.gov/projects/ransomware-protection-and-response
- ✓ **NIST SMALL BUSINESS CYBERSECURITY CORNER:** https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware
- ✓ **TIPS & TACTICS SHEET:** https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

QUESTIONS? Email us: ransomware@nist.gov

Last Updated: February 2022

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