TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Controls to Prevent and Recover From Ransomware Attacks Were Generally Effective

November 23, 2022

Report Number: 2023-20-002

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Controls to Prevent and Recover From Ransomware Attacks Were Generally Effective

Final Audit Report issued on November 23, 2022 **Report Number 2023-20-002**

Why TIGTA Did This Audit

Ransomware is a type of cyber extortion where an attacker uses a form of malware to hold computer systems or networks hostage until the owner pays a ransom. Global ransomware attacks have increased rapidly, almost tripling from the beginning of Calendar Year 2019 to the end of Calendar Year 2020, with over 100 million attacks in the last quarter of Calendar Year 2020 alone.

This audit was initiated to determine the effectiveness of controls to respond to and recover from malware (ransomware) attacks.

Impact on Tax Administration

As the Nation's tax agency, the IRS collects and stores substantial amounts of Personally Identifiable Information, including all tax records for individuals, corporations, *etc.* In addition, IRS systems contain information about planned or ongoing examinations, collection actions, and criminal investigation cases.

A successful ransomware attack could significantly impact tax administration and possibly national security. The IRS uses hundreds of different computer systems to perform different functions, from storing tax records to consolidating print files for notices. Depending on which systems are infected, the result could vary from minor to catastrophic.

What TIGTA Found

TIGTA reviewed IRS policies and procedures related to Incident Response Plan requirements and determined they were generally consistent with National Institute of Standards and Technology guidance.

IRS officials state there have been no successful ransomware attacks against the IRS prior to June 2022. However, the IRS informed TIGTA of one unsuccessful ransomware attack that was identified and mitigated. [redacted]. The IRS identified website traffic patterns consistent with ransomware and removed the computer from the network. For this attack, TIGTA determined that the IRS took appropriate actions to resolve the incident.

TIGTA also reviewed IRS policies and procedures related to required alternate storage site and system backup contingency planning controls and determined they were generally consistent with National Institute of Standards and Technology guidance.

In addition, TIGTA selected four information systems and reviewed the results of annual testing of their Information System Contingency Plans from July 1, 2021, through June 30, 2022. For three of the information systems, the IRS completed required testing and did not identify any issues related to alternate storage sites and system backups. Accordingly, TIGTA concluded that these systems had effective controls to enable them to be restored in the event of a ransomware attack. The test results for the fourth information system identified unresolved issues related to the failure to backup system data on a daily basis as required. During our audit, the IRS corrected these deficiencies by performing daily backups, but system data were at risk for approximately two years until the IRS addressed the deficiencies.

What TIGTA Recommended

TIGTA made no recommendations as a result of the work performed during this audit. In its response to the report, the IRS agreed with the facts and conclusions presented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

November 23, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Controls to Prevent and Recover From Ransomware Attacks Were Generally Effective (Audit # 202220006)

This report presents the results of our review to determine the effectiveness of controls to respond to and recover from malware (ransomware) attacks. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS [Internal Revenue Service] Resources.*

Management's complete response to the draft report is included as Appendix II.

Copies of this report are also being sent to the IRS managers affected by the information in the report. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

Malware is a general term used to refer to types of computer programs that are designed to disrupt, damage, or gain unauthorized access to computers in order to cause disruption for financial or political gains. Common types of malware include viruses, worms, Trojans, spyware, and ransomware, each of which have unique characteristics.

Ransomware is a type of cyber extortion where a form of malware infiltrates computer systems or networks and encrypts data, holding it 'hostage' until the victim pays a ransom. The attacker informs the victim that their data are encrypted and in order to decrypt the files, the victim has to pay a sum of money. However, even if the victim pays the ransom there is no guarantee that the attacker will follow through and decrypt the files.

Global ransomware attacks have rapidly increased, more than tripling from the beginning of Calendar Year 2019 to the end of Calendar Year 2020, with over 100 million attacks in the last quarter of Calendar Year 2020 alone. Ransomware attacks have progressed from simple extortion to include exfiltration of data, which enables the attackers to distribute the information online to embarrass or destroy reputations. Further, nation-states[1] are using ransomware to encrypt data to prevent it from being used and to cause disruption, rather than for profit. Finally, it has become so common that there is a Ransomware as a Service model, where bad actors rent out their services.

An example of the danger from ransomware is the attack on the Colonial Pipeline energy company in May 2021. At the time, the company carried 2.5 million barrels of oil per day in its pipelines and provided 45 percent of the East Coast's fuel supply. Using ransomware, hackers encrypted 100 gigabytes of sensitive data and held the data hostage, which forced the company to freeze its information technology systems and shut down operations for six days. The company paid $4.4 million to recover the data. This attack not only cost the company financially, but also affected the price of gas nationwide.

A ransomware attack starts when an exploit is used to enable a specific type of malware (the 'payload') to be inserted into the network. By far, the primary attack vector is through phishing; the ransomware payload is activated when an attachment is opened or a link clicked. Additional examples of attack vectors include remote attacks on the network, misconfigured cloud services, and via remote access protocols.

Once in the network, the ransomware code identifies ways to propagate through the network and attempts to escalate privileges to gain administrator rights. It also attempts to establish contact with a command and control server run by the attackers. Finally, after mapping the network as much as possible, it encrypts specific data and alerts the victim. However, the process is constantly evolving as network security tools identify and stop common methods.

As the Nation's tax agency, the Internal Revenue Service (IRS) collects and stores substantial amounts of Personally Identifiable Information, including all tax records for individuals, corporations, *etc*. In addition, IRS systems contain information about planned or ongoing examinations, collection actions, and criminal investigation cases. A successful ransomware

[1] See Appendix III for a glossary of terms.

attack could have a very significant impact on tax administration and possibly national security. The IRS uses hundreds of different computer systems to perform various functions, from storing tax records to consolidating print files for notices. Depending on which systems are infected, the result could vary from minor to catastrophic.

Federal agencies are required to implement network security controls developed by the National Institute of Standards and Technology (NIST) to help ensure that their networks are secure. NIST guidance specifies security controls for organizations and information systems that support the executive agencies of the Federal Government to ensure that they meet the minimum requirements of the Federal Information Processing Standards Publication 199.[2] These guidelines apply to all components of an information system that process, store, or transmit Federal information.

Specific types of NIST controls apply to preventing, mitigating, and recovering from malware. Prevention controls include firewalls, intrusion detection, and monitoring controls. However, due to the rapid change in the cyber threat landscape, new versions of malware are constantly being introduced, some of which may not be identified or mitigated by preventive controls. Experts agree that having the system and user data backed up frequently and securely is one of the single most important things that an organization can do to mitigate a successful ransomware attack, so the organization can restore data if the original data are lost.

Results of Review

Policies and Procedures Related to Incident Response Plan Requirements Were Generally Consistent With National Institute of Standards and Technology Guidance

NIST Special Publication 800-53, Revision 5,[3] contains the requirements for developing, distributing, updating, communicating, and protecting an Incident Response Plan. This guidance emphasizes the importance for organizations to develop and implement a coordinated approach to incident response. Further, it requires the development of an Incident Response Plan that complies with key items to include defining reportable incidents, providing metrics to measure the organization's incident response capabilities, and sharing of incident information.

We reviewed information in the Internal Revenue Manual (IRM)[4] specific to establishing an Incident Response Plan and compared it to the NIST Special Publication previously cited and determined that the IRM is generally consistent with the NIST requirements.

[2] NIST, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

[3] NIST, Special Publication 800-53 (Rev. 5), *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

[4] IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance* (Sept. 2021).

One Ransomware Attack Was Mitigated by Properly Applying Incident Response Procedures

NIST Special Publication 800-61, Revision 2,[5] states that incidents can occur in countless ways, so it is not feasible to develop step-by-step instructions for handling every incident. However, organizations should generally be prepared to handle any incident and should focus on being prepared to handle incidents that use common attack vectors like web based, e-mail, or removable media. Different types of incidents merit different response strategies. For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents and determining whether an incident has occurred.

The IRS's Computer Security Incident Response Center (CSIRC) provides daily operational coverage for monitoring and analysis for intrusion attempts or anomalous activity. The CSIRC Incident Response Plan states that incidents identified by or reported to the CSIRC are assessed to determine the nature and severity of events to formulate a prompt response for containment and eradication, thereby minimizing impact. Reported incidents are documented within the CSIRC centralized Incident Tracking System and further triaged to determine the validity, severity, and impact of the event.

The CSIRC uses an incident management playbook containing specific actions necessary throughout the incident management lifecycle to mitigate a detected incident. One section of the playbook provides detailed steps to eradicate malicious code, which includes ransomware. NIST defines malware as malicious code and ransomware is a type of malware.

CSIRC officials stated that there have been no successful ransomware attacks against the IRS prior to June 2022. However, the CSIRC informed us of one unsuccessful ransomware attack which occurred in May 2022. [redacted]. CSIRC personnel analyzed the website browsing log and identified website traffic patterns consistent with ransomware, and then removed the computer from the network. We compared the details of this incident response report against current policies and procedures and determined that the CSIRC took appropriate actions to resolve the incident.

Policies and Procedures Related to Alternate Storage Site and System Backup Controls Were Generally Consistent With National Institute of Standards and Technology Guidance

NIST Special Publication 800-34, Revision 1,[6] is devoted to contingency planning for Federal information systems and includes guidelines for Federal agencies to follow. Information systems are vital elements in most organizations and are essential to an organization's success. It is critical that services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each

[5] NIST, Special Publication 800-61 (Rev. 2), *Computer Security Incident Handling Guide* (Aug. 2012).

[6] NIST, Special Publication 800-34 (Rev. 1), *Contingency Planning Guide for Federal Information Systems* (May 2010).

system providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

The IRS is completely restructuring the July 2021 version of IRM 10.8.60[7] to align it with the Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directives 1 and 2.[8] The IRS plans to rename this IRM to *Business Impact Analysis (BIA) Policy and Guidance* and only include polices related to Business Impact Analysis.

Information System Contingency Plan (ISCP) testing policies and Contingency Planning control information previously contained in IRM 10.8.60 were moved to other sources, primarily IRM 10.8.62[9] and IRM 10.8.1. These updates ensured that the IRS has a policy in place that requires testing of the ISCPs or Disaster Recovery plans to determine its capability to recover and restore its systems in the event of a disruption, disaster, or catastrophe. We reviewed information in these IRMs specific to alternate storage site and information system backup controls, as well as testing requirements, and compared them to the information in the NIST Special Publication.

We determined that the policies and procedures in the IRMs previously referenced were generally consistent with NIST Special Publication 800-34, Revision 1, contingency planning guidance to establish controls when developing, deploying, and operating information systems, as well as testing requirements for those controls.

Contingency Planning Controls Related to Backups Were Generally Effective Based on Annual Testing Results

The IRM establishes the security framework for the development of security control-specific implementations defined in the IRMs, IRS publications, and other procedural guidance. The Security Risk Management office is responsible for the annual testing of NIST controls for all systems, as well as coordinating and providing information to external stakeholders regarding the status of meeting annual Federal Information Security Modernization Act of 2014[10] requirements. Federal law, specifically the Federal Information Security Modernization Act of 2014, requires agencies to test contingency planning security controls.

One IRM requirement for contingency planning controls is that systems are required to have an ISCP document and associated ISCP Testing Checklists. An ISCP Testing Checklist provides a step by step process to guide participants through the annual testing requirements for the ISCP. For example, it specifies the scope of various tests, such as restoring a system by retrieving backup data from an alternate storage site and restoring the data to test its usability. IRS

[7] IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance,* (July 2021).

[8] U.S. Department of Homeland Security, Federal Emergency Management Agency, *Federal Continuity Directive 1* (Jan. 2017) and U.S. Department of Homeland Security, Federal Emergency Management Agency, *Federal Continuity Directive 2* (June 2017).

[9] IRM 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program,* (Feb. 2022).

[10] Public Law 113-283. It provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

system owners develop these ISCP documents to provide information devoted to all aspects of contingency planning for individual systems.

The types and frequency of tests being performed are determined using NIST criteria. In addition, the Federal Information Processing Standards Publication 199 provides the Standards for Security Categorization of Federal Information Systems. The IRS categorizes the security impact level, based on the confidentiality, integrity, and availability of a system, as either Low, Medium, or High.

Systems designated as Low are required to have a Tabletop Exercise and Functional Exercise annually, while those that are Medium are required to have a Tabletop Exercise annually and a Functional Exercise twice a year. High level systems require a Tabletop Exercise and four Functional Exercises each year, as well as a Disaster Recovery Exercise. The type of test most applicable to our objective was Functional Testing, because it includes real world testing of the backup process documented in the ISCP. System owners work with staff from the Enterprise Operations function's Data Management and Services Support Division to conduct functional testing and provide evidence of the test results to the Cybersecurity function's ISCP Testing group.

We selected a judgmental sample[11] of four information systems from the following business operating divisions: Criminal Investigation, the Information Technology organization, and the Small Business/Self-Employed and Wage and Investment Divisions. For each of the four sample information systems, we reviewed the most recent annual ISCP functional testing results from July 1, 2021, through June 30, 2022, including the ISCP document created by the system owner and ISCP Testing Checklist(s) and testing documentation.

For three (75 percent) of the four sample information systems, we did not identify any issues related to alternate storage site and system backup controls identified during functional testing. Based on this, we concluded that these systems had effective controls to enable them to be restored in the event of a ransomware attack. However, the fourth information system had issues related to system backups.

Issues with contingency planning controls were previously identified for one sample system

The IRM requires the IRS to perform daily backups of system data for a system categorized as High. We identified that one of the four sampled information systems had unresolved issues related to the failure to backup system data on a daily basis as required. This issue was identified during annual control testing in Calendar Year 2020, and it involved four components of the main system. The system owner created a Plan of Action and Milestones for each of the four affected components, documenting the control weakness and planned remedial actions to correct it. The time assigned to correct the weaknesses was two years, with a due date of May 2022.

We determined that these Plans of Action and Milestones were closed by the May 2022 due date. Even though the IRS timely closed these Plans of Action and Milestones, the control weakness was still present on the system for approximately two years. If there had been an

[11] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

emergency requiring a system restore, such as a ransomware attack, the most current data would not have been available for system restoration.

The situation described illustrates the potential risk created by inadequate backup controls. During a discussion with IRS management, they agreed that the system data were at risk for the entire time until they addressed the deficiencies. This is particularly concerning as the system was rated with a Security Impact-Level of High, which represents the most important systems.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine the effectiveness of controls to respond to and recover from malware (ransomware) attacks. To accomplish our objective, we:

- Reviewed Federal Government and IRS requirements for an incident response plan, an alternate storage site, and information system backup controls.
- Determined whether the controls for incident response related to malware, specifically ransomware, were effective by comparing the details of one incident response report against IRS policies and procedures.
- Determined whether the alternate storage site and information system backup controls of systems potentially affected by malware, specifically ransomware attacks, were effective by interviewing IRS management and personnel and reviewing ISCP testing results from July 1, 2021, through June 30, 2022. We reviewed ISCP testing results for a judgmental sample[1] of four information systems from a list of 157 information systems. A judgmental sample was used because we did not plan to project the results to the population.
- Determined whether the system owner(s) created a Plan of Action and Milestones to address any deficiencies identified during ISCP testing.

Performance of This Review

This review was performed during the period November 2021 through September 2022. Due to the ongoing Coronavirus Disease 2019 pandemic, we conducted all audit work virtually. We held meetings and interviews via teleconference. We worked closely with the Cybersecurity function, including the Cyber Operations and Security Risk Management offices, and the Enterprise Operations function. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Joseph Cooney, Audit Manager; Ashley Weaver, Lead Auditor; and Steven Stephens, Senior Auditor.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

following internal controls were relevant to our audit objective: NIST requirements for security and privacy controls, contingency planning, computer security incident handling for Federal information systems, and the NIST Federal Information Processing Standards Publication; and IRS policies and procedures related to information technology security controls, the Incident Response Plan, and the CSIRC incident management playbook. We evaluated these controls by interviewing IRS employees and analyzing relevant documentation provided by the IRS.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

November 3, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger, Chief Information Officer Nancy A. Sieger Digitally signed by D3CCB Date: 2022.11.03 15:32:20 -04'00'

SUBJECT: Draft Audit Report – Controls to Prevent and Recover From Ransomware Attacks Were Generally Effective (Audit #202220006)

Thank you for the opportunity to review your draft audit report and address the report observations with the audit team. We agree with your team's observation that the IRS has effective controls in place to prevent and recover from ransomware attacks. One of my priorities as Chief Information Officer is to ensure that the IRS can defend against ransomware attacks and recover quickly in the event of any cyber-related incident.

The IRS Cybersecurity function, including our Computer Security Incident Response Center and Cyber Threat Fusion Center, focuses on staying one step ahead of potential threats. As part of the government-wide effort, we continuously coordinate with the Department of the Treasury and the Cybersecurity and Infrastructure Security Agency. Malicious cyber actors intent on disrupting U.S. government operations, through the use of ransomware attacks, remain a persistent threat; however, as this report indicates, the controls we have in place today are working as intended to maintain the confidentiality, integrity, and availability of IRS information and systems.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Richard Therrien, Director of Cybersecurity Operations, at (240) 613-5262.

Appendix III

Glossary of Terms

Term	Definition
Alternate Storage Site	A site geographically distinct from primary storage sites that maintain duplicate copies of information and data if the primary storage site is not available.
Attack Vector	A path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information.
Backup	The process of duplicating and storing the files and programs of an information technology system on another medium or device to facilitate complete restoration of the system and its data following a disruption.
Business Impact Analysis	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Business Operating Division	A title for major IRS organizations such as the IRS Independent Office of Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and Information Technology.
Computer Security Incident Response Center	Part of the Cybersecurity function. Its mission is to ensure that the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyber threats or cyber-attacks. One of the primary duties of the CSIRC is to perform 24-hour monitoring and support to IRS operations seven days a week, 365 days a year. In addition, the CSIRC coordinates potential cybercrimes with the Treasury Inspector General for Tax Administration's Office of Investigations, Electronic Crimes and Intelligence Division, for further investigation and legal proceedings.
Contingency Planning	The process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively affects the organization.
Cybersecurity Function	Within the Information Technology organization, it is responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of information or a system. In addition, an incident could constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyberattacks against an organization's information systems.

Term	Definition
Information System Contingency Plan	Documents created and maintained by the Cybersecurity function and system owners that provide procedures and capabilities for recovering an information system and define the resources, roles, responsibilities, and procedures for recovering a single information system after a disruption.
Malicious Code	Software designed to infiltrate or damage a computer system without the owner's informed consent.
Nation-State	A form of political organization in which a group of people who share the same history, traditions, or language live in a particular area under one government.
National Institute of Standards and Technology	A nonregulatory Federal agency within the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Network	An information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of Personally Identifiable Information are: name, Social Security Number, date of birth, place of birth, address, and biometric record.
Plan of Action and Milestones	A requirement for managing the security weaknesses pertaining to a specific application or system. In addition to noting weaknesses, each Plan of Action and Milestones item details steps that need to be taken to correct or reduce any weaknesses, as well as resources required to accomplish task milestones and a correction timeline.
Security Risk Management	An office within the Cybersecurity function that provides guidance and direction to the IRS enterprise-wide disaster recovery efforts, as well as a comprehensive, business-centric information technology service continuity management program designed to protect IRS operations, assets, and information.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.
System Owner	The agency official responsible for the overall procurement, development, integration, modification, operation, and maintenance of the information system. Also known as the Business and Functional Unit Owner.

Appendix IV

Abbreviations

CSIRC	Computer Security Incident Response Center
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISCP	Information System Contingency Plan
NIST	National Institute of Standards and Technology

To report fraud, waste, or abuse,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589