NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
Cyber Center
Cyber Advisory
17 March 2020 | Product No. 2020-03-023
NTIC SIN No. 2.5 | HSEC SIN No.1.8

Healthcare and Public Health Sector Organizations at High Risk of Cyber Attacks Exploiting COVID-19 Pandemic

TLP: GREEN | ***The NTIC Cyber Center assesses with high confidence that organizations within the Healthcare and Public Health Sector are at high risk of targeted and opportunistic cyber attacks exploiting the COVID-19 pandemic to disrupt operations, steal sensitive data, and generate illicit revenue for profit-motivated cyber threat actors.***

Over the past several years, Healthcare and Public Health Sector organizations have become increasingly attractive targets for cyber threat actors not only because of the treasure trove of sensitive personal and medical data collected and stored on their servers, but also because of the critical functions they perform. Unauthorized access of sensitive data and the disruption of operations can have a devastating and debilitating effect on those in need of the life-sustaining services these organizations provide. Historically, successful cyber attacks launched against organizations within this sector have resulted in stolen, inaccessible, or destroyed patient electronic health information, the unavailability of organization websites, servers, and email systems, disabled or disrupted telephone communications, and the cancellation or delay of scheduled medical procedures and other appointments.

As the rapid emergence of COVID-19 within the US has already begun to place a strain on healthcare facilities, disruptive and destructive cyber attacks could potentially delay or cease critical services as the demand for COVID-19 testing and treatment increases. To reduce the risk of this scenario occurring, the NTIC Cyber Center urges cybersecurity professionals and IT administrators working in the Healthcare and Public Health Sector to take steps now to secure their networks and devices against cyber attacks. To assist in this effort, we are providing this product to highlight cyber threats that are likely to impact this sector, along with additional resources cybersecurity teams and healthcare staff can reference to reduce risk.

Cyber Threats Most Likely to Impact the Healthcare and Public Health Sector

Ransomware: a type of malicious software (malware) designed to extort money from victims by restricting access to a computer, mobile device, or digital files. The most common attack vectors ransomware operators use to infect networks include malicious attachments and links in emails, Remote Desktop Protocol (RDP) compromise, compromise of managed service providers (MSPs), and exploit kits on compromised and malicious websites. ***Please see the included NTIC Cyber Center Ransomware Mitigation Guide for more information on how to protect systems and networks from this threat.***

- In 2019, ransomware impacted 764 healthcare providers nationwide, with healthcare organizations among the top three sectors most commonly targeted by ransomware in the United States.[i]

- On Tuesday, March 10, 2020, a ransomware attack impacted an Illinois public health agency, disabling its main website and restricting employees' access to medical files.[ii]

- On Friday, March 13, 2020, computer systems at the University Hospital Brno in the Czech Republic were disabled after a cyber attack. Although details of the attack have yet to be released, cybersecurity experts believe it was likely the result of a ransomware attack. This attack delayed COVID-19 test results and prevented collected medical data from being stored in databases.[iii]

Social Engineering: a psychological technique used by cyber threat actors to trick victims into performing actions against their best interest, or the interest of their organization. The most common forms of social engineering include phishing, spear phishing, whaling, vishing (voice phishing), and domain name and email spoofing. These methods are used to steal login credentials, obtain financial and other sensitive data, and infect victims with malware.

- In February 2020, a cyber security company observed several COVID-19-related email phishing campaigns spoofing official correspondence from known entities. These campaigns featured messaging advertising a secret cure for the virus, masquerading as an internal email from a business organization's president, and impersonating health authorities such as the World Health Organization. Many of these emails included links to spoofed websites designed to trick email recipients into surrendering user credentials for services by DocuSign, Microsoft Office 365, and Adobe. Other emails contained malicious attachments that, when opened, install the NanoCore remote access Trojan to grant an attacker full control over a compromised system or the AgentTesla keylogger to record keystrokes and steal banking and financial information from victims.[iv]

- In February 2020, an antivirus company observed COVID-19-related phishing emails disguised as correspondence from the Centers for Disease Control, advice from medical experts on how to protect against the virus, and human resources policies outlining organizational procedures for workplaces.[v]

- In March 2020, security researchers discovered malicious code embedded in a website hosting a fraudulent copy of Johns Hopkins University's interactive COVID-19 heatmap. The website, registered in February 2020 using Russian nameservers, hid a variant of AzorUlt spyware that was capable of skimming visitors' passwords and payment card details as well as deploying other malware. As of the time of writing, the website has not been observed in any known malicious email campaigns; however, it is believed that the threat actors have relied on organic visitor traffic to the website to propagate the information-stealing malware contained on the webpage.[vi]

Distributed Denial-of-Service (DDoS): the overwhelming of a target or its surrounding infrastructure with a flood of Internet traffic to cause the disruption of a service or network. DDoS attacks are commonly launched using a network of infected systems or devices instructed by a command-and-control (C2) server to send network traffic to a particular target. An unintended DDoS condition can also occur when many people, applications, or systems attempt to gain access to a single system or service at the same time.

- After a DDoS attack impacted Boston Children's Hospital in 2014, the Center for Internet Security (CIS) released an advisory promoting a Multi-State Information Sharing and Analysis Center (MS-ISAC) guide for mitigating DDoS attacks.[vii]

- In 2017, the US Federal Bureau of Investigation released a Public Service Announcement that included guidance for securing Internet-of-Things (IoT) devices, including medical devices, against compromise that could lead to DDoS attacks.[viii]

- In 2018, cybersecurity firms reported an increase in DDoS attacks targeting healthcare organizations, prompting many organizations to consider implementing DDoS mitigation and management services.[ix]

- On March 15, 2020, the US Department of Health and Human Services (HHS) experienced a cyber attack that was likely a DDoS attack, according to multiple sources. HHS reported that, although they detected a "significant increase in activity on HHS cyber infrastructure," their network remained "fully operational."[x]

Telephony Denial-of-Service (TDoS): the attempt to make a targeted telephone system unavailable to legitimate incoming or outgoing calls by flooding it with call traffic or compromising a Voice-over-IP (VoIP) system. TDoS attacks are commonly launched against public safety answering points (PSAPs) and emergency call centers. An unintended TDoS condition can also occur when many people attempt to call a phone number at the same time, or a malicious mobile application generates a high volume of outgoing calls without the mobile phone user's interaction.

- In 2018, security researchers assessed that it only takes approximately 6,000 smart phones to disable 9-1-1 emergency services or PSAPs.[xi]

Recommendations

The NTIC Cyber Center recommends cybersecurity professionals and IT administrators within the Healthcare and Public Health Sector review the following mitigation strategies and included guides to help reduce their organizations' risk of a potentially crippling cyber attack.

- Educate all staff about the increasing risk of malicious emails and websites exploiting the COVID-19 pandemic to steal data and deliver malware to unsuspecting victims and encourage them to report any suspicious emails or network activity immediately.

- Remind staff about the importance of using lengthy, complex, and unique passwords for each account and enforce the use of multifactor authentication, if available.

- Apply all available security patches and updates to systems, devices, and software after appropriate testing.

- Consider tightening firewall settings and whitelisting only pre-approved websites and IP addresses to prevent users from accidentally visiting a malicious URL.

- Conduct an audit of your network to identify all systems, devices, and services and limit exposure of that network to the network.

- If possible, segregate critical systems and devices on separate, isolated networks to reduce the impact of a malware infection.

- Backup critical data daily, keep it stored off the network in a secure location, and regularly test backups and backup procedures to reduce recovery time should a ransomware attack or other destructive malware attack occur.

- Regularly audit user accounts for unauthorized privilege escalation and immediately deactivate unneeded or unused accounts. Deactivate staff accounts immediately upon termination or departure of an end user.

- Regularly audit all external access to networks by MSPs, contractors, and other external parties.

- Contact any MSPs and ask what strategies they have in place to prevent MSP account compromise.

- Consult your legal team and insurance companies for additional guidance appropriate for your organization.

Additionally, the NTIC Cyber Center advises cybersecurity professionals and IT administrators within the Healthcare and Public Health Sector to review the following strategies to defend against, respond to, and mitigate the effects of TDoS attacks:

Prior to a TDoS attack

- Prepare a response plan for managing communication and coordination efforts during a TDoS attack.

- Discuss protocols for monitoring and responding to TDoS attacks with your telephone service provider.

- Isolate critical phone system lines from those serving non-critical or administrative functions. In addition, prevent the rollover of calls placed to non-critical lines from transferring to critical phone lines.

- Implement backup communication methods such as mobile smartphones or a virtual phone system that can be activated during a TDoS attack if needed.

- Use strong and unique passwords on phone and computer systems to reduce risks of abuse, hacking, or other malicious activity.

- Work with third party vendors to implement systems that divert unwanted phone traffic and allow legitimate traffic to connect without interruption.

During a TDoS attack

- Log all incoming phone numbers, IP address traffic, the start and stop times of events, and the number and frequency of calls received.
- Save voice recordings of any calls placed before, during, or after a TDoS attack. If a caller demands payment, record any instructions given on how to pay, including account numbers or call-back phone numbers.
- Monitor network security for any malicious cyber activity that may take place during a TDoS attack.

After a TDoS attack

- Report the attack to local law enforcement, the National Cybersecurity and Communications Integration Center, and the FBI's Internet Crime Complaint Center.
- Compile all call and IP logs and save for long-term retention.

---

[i] (U); Emsisoft; "The State of Ransomware in the US: Report and Statistics 2019"; 12 DEC 2019; https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/; accessed on 13 MAR 2020.

[ii] (U); Benjamin Freed; Statescoop; "Amid Coronavirus Scare, Ransomware Targets Public Health Agency in Illinois"; 12 MAR 2020; https://statescoop.com/amid-coronavirus-scare-ransomware-targets-public-health-agency-illinois/; accessed on 13 MAR 2020.

[iii] (U); Ionut Ilascu; Bleeping Computer; "COVID-19 Testing Center Hit by Cyber Attack"; 14MAR 2020; https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/; accessed on 13 MAR 2020.

[iv] (U); Sherrod DeGrippo; Proofpoint; "Attackers Expand Coronavirus-Themed Attacks and Prey on Conspiracy Theories"; 13 FEB 2020; https://www.proofpoint.com/us/corporate-blog/post/attackers-expand-coronavirus-themed-attacks-and-prey-conspiracy-theories; accessed on 13 MAR 2020.

[v] (U); Steve Symanovich; Norton; "Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams"; published date unknown; https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html; accessed on 13 MAR 2020.

[vi] (U); David Ruiz; Malwarebytes Labs; "Battling Online Coronavirus Scams with Facts"; 10 MAR 2020; https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/; accessed on 13 MAR 2020.

[vii] (U); Center for Internet Security; "DDoS Attacks: In the Healthcare Sector"; published date unknown; https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/; accessed on 13 MAR 2020.

[viii] (U); FBI; I-101717a-PSA; "Common Internet of Things Devices May Expose Consumers to Cyber Exploitation;" 17 OCT 2017; https://www.ic3.gov/media/2017/171017-1.aspx; accessed on 13 MAR 2020.

[ix] (U); Fred Donovan; Hit Infrastructure Corporation; "Healthcare DDoS Attacks on Organizations Edged Up in 2018 Telephony Denial of Service (TDoS) Threat"; 21 MAR 2019; https://securelogix.com/wp-content/uploads/2019/06/TDoSWhitePaper.pdf; accessed on 15 MAR 2020.

[x] (U); Sara Morrison; Vox; "What We Know about the Health Department Website Cyberattack"; 16 MAR 2020; https://www.vox.com/recode/2020/3/16/21181825/health-human-services-coronavirus-website-ddos-cyber-attack ; accessed on 17 MAR 2020.

[xi] (U); Carl Herberger; Security Boulevard; "It Only Takes 6,000 Smart Phones to Take Down Our Public Emergency Response System?"; 28 JUN 2018; https://securityboulevard.com/2018/06/it-only-takes-6000-smart-phones-to-take-down-our-public-emergency-response-system/; accessed on 13 MAR 2020.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
Cyber Center
Cyber Advisory

The NTIC Cyber Center Ransomware Mitigation Guide

TLP: **WHITE** | ***Ransomware is a type of malicious software (malware) designed to extort money from victims by restricting access to a computer, mobile device, or digital files.*** The most common form of this malware is crypto-ransomware, which uses an encryption process to render devices and files unusable until a decryption key is obtained by the victim. Indiscriminate ransomware infections most often occur because an unsuspecting victim opened a malicious email attachment, clicked on a poisoned link in an email, or visited a compromised website. Targeted ransomware attacks are commonly deployed manually by a cyber threat actor after he or she gains unauthorized access to a system or server on a network. While ransomware attacks cannot completely be prevented, the risk and impact of this type of malware infection can be dramatically reduced by implementing the following cybersecurity strategies and improving cybersecurity awareness within your organization. *(The NTIC Cyber Center provides the following list for informational purposes and does not endorse any specific commercial products, processes, or services.)*

Data Management

- Schedule data backups often and ensure they are kept offline in a separate and secure location. Initially perform a full backup and then conduct either incremental, differential, or mirror backups depending on your organization's needs and capabilities. Consider maintaining multiple backups in different locations for redundancy. Test backups regularly to ensure their integrity.
- If an online backup and recovery service is used, contact the service provider immediately after a ransomware infection is suspected to prevent the malware from overwriting previous file versions with the newly encrypted versions.

System Management

- Use reputable antivirus software and ensure that it is activated and updated with the latest malware definitions. Schedule scans as often as permitted.
- Enable automated patching for operating systems, software, plugins, and web browsers.
- Follow the Principle of Least Privilege for all user accounts and enable User Access Control (UAC) to prevent unauthorized changes to user privileges. Regularly audit user accounts and disable or delete those that are no longer in use.
- Implement application whitelisting to prevent unauthorized or malicious software from executing.
- Turn off unused wireless connections.
- Disable macros on Microsoft Office software.
- Use reputable ad blocking extensions in browsers to prevent "drive-by" infections from advertisements containing malicious code.
- Disable the ***vssadmin.exe*** tool by renaming it to prevent ransomware from deleting Shadow Volume Copies. Instructions on how to rename this tool are included here.
- Disable Windows Script Host and Windows PowerShell.
- Disable Remote Desktop Protocol (RDP), Telnet, and SSH connections on systems and servers if it is not needed in your environment. Block inbound traffic to associated ports.
- If remote access is needed, audit access, whitelist authorized IP addresses, ensure that login credentials are complex, and implement a multifactor authentication solution to prevent unauthorized access.

- Use web filtering tools to block access to malicious websites. Scan all incoming emails, attachments, and downloads and configure email servers to proactively block emails containing suspicious attachments such as ***.exe***, ***.vbs***, and ***.scr***.
- Configure systems by modifying the Group Policy Editor to prevent executables (***.exe***, ***.rar***, ***.pdf***, ***.exe***, ***.zip***) from running in ***%appdata%***, ***%localappdata%***, ***%temp%*** and the Recycle Bin.
- *Implement a behavior blocker to prevent ransomware from executing or making any unauthorized changes to systems or files.
- *Consider utilizing a free or commercially available anti-ransomware tool offered by leading computer security vendors.
- *To counteract ransomware variants that modify the Master Boot Record (MRB) and encrypt the Master File Table (MFT), Cisco Talos has released a Windows disk filter driver called MBRFilter, available on GitHub here.
- *For macOS X users, a free tool called *RansomWhere?* is available to monitor for and prevent ransomware infections. Information about this tool is available on the Objective-See website here and the tool itself can be downloaded here.

**The NTIC Cyber Center recommends exercising caution before downloading any software from the internet, scanning associated files for malware prior to installation, and testing them in a staging environment prior to performing a large-scale deployment.*

Network Management

- Set a network performance baseline for network monitoring prior to an infection to improve your ability to detect anomalies and malicious activity.
- Ensure your firewall is enabled and properly configured.
- Close and monitor unused ports.
- Disable SMBv1 on firewall and all systems on the network.
- Block inbound traffic to TCP/UDP ports 139 and TCP port 445.
- Block known malicious Tor IP addresses. A list of active Tor nodes updated every 30 minutes can be found here.
- Perform vulnerability scans against your organization's IP address range(s) regularly to identify poorly configured and vulnerable internet-facing systems and take the appropriate corrective actions as needed.
- Keep network log files for a full year in the event a ransomware or other network intrusion incident leads to a criminal investigation.

Mobile Device Management

- For Apple iOS devices: ensure data is backed up on iCloud and two-factor authentication is enabled, only download media and apps from the official App Store, and avoid "jailbreaking" the device.
- For Android devices: disable the "unknown sources" option in the Android security settings menu, install apps only from the official Google Play store after carefully reading the associated ratings and reviews, and avoid "rooting" the device.

How to quickly contain a ransomware infection:

- Immediately unplug the Ethernet network cable or disable Wi-Fi on the infected system. This will prevent the ransomware from spreading to other systems on the network or infecting backups that are stored on the network or in a cloud environment. Immediately quarantine the infected system and do not reconnect it to the network until it has been thoroughly scanned and cleaned.
- Alternatively, instruct employees to turn off the power or unplug the power cord from the system. Although doing so may hinder a complete forensic analysis of the infected system, it stops the encryption process and may limit data loss.
- Employees should notify the appropriate information security contact within your organization as quickly as possible.

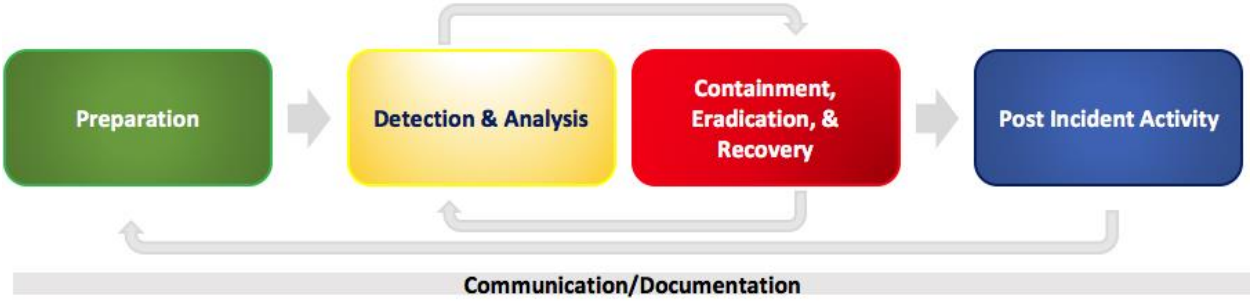
How to recover after a ransomware infection has occurred:

- Locate backups of the affected data or system that predate the infection (to avoid restoring an infected instance), restore the data, and harden the system and network against future infections.
- If no viable backups are available, conduct an online search of the ransomware variant to see if there is a publicly available decryption tool or remediation method. *No More Ransom!* is one online resource that provides guidance to victims and free decryption tools for a number of variants. Victims are also encouraged to submit an incident report to the NTIC Cyber Center at ncrintel.org and an analyst may be able to provide additional assistance.
- If no decryption tool is available, the only remaining options are to accept the data loss or pay the ransom. The NTIC Cyber Center discourages paying ransoms of any kind, as this perpetuates the crime and does not guarantee data recovery. Additionally, organizations that send ransom payments to known sanctioned individuals may be subject to secondary sanctions, fines, or face other legal ramifications according to a November 2018 press release by the US Department of the Treasury's Office of Foreign Assets Control (OFAC).
- After removing the malware and restoring the machine, change all system, network, and online account passwords and implement the mitigation recommendations provided in this document.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
Cyber Center
Cyber Advisory

The NTIC Cyber Center Guide for Cyber Incident Response Planning

TLP: **WHITE** | This guide is provided to assist organizations in preparing for a cyber-attack that could negatively impact the confidentiality, integrity, or availability of their data. Implementing a comprehensive cyber incident response plan can greatly aid organizations by minimizing damage to equipment and reducing disruption to business operations. The following is an introduction to the four phases of the Cybersecurity Incident Lifecycle, which characterizes the continuous efforts organizations make to handle incidents and ensures continuous improvements in their overall security posture.



1. **Preparation**
   - Develop an incident response policy, approved by the highest level within your organization, that contains the following key elements:
     - Statement of management commitment
     - Purpose and objectives
     - Scope (to whom and what it applies and under what circumstances)
     - Definitions of computer security incidents and related terminology
     - Organizational structure and definition of roles, responsibilities, and level of authority
     - Prioritization or severity ratings of incidents
     - Performance measures
     - Reporting and contact forms
   - Develop standard operating procedures (SOPs) based on your incident response policy and relative to the specific technical processes, techniques, checklists, and forms to be used by your cyber security incident response team (CSIRT).
   - Assign staff to your organization's CSIRT, ensuring that each staff member acknowledges and understands your organization's policy and procedures relevant to his or her role and level of authority within the team.
     - In addition to core members responsible for directly responding to incidents, CSIRTs should also include technical subject matter experts, IT support staff, legal counsel, human resources, public relations staff, and senior management. *Smaller organizations that choose to outsource some or all of the CSIRT roles to an incident response provider should still maintain an internal policy and plan for early stage incident response before the provider's team arrives.*
     - Designate an incident leader who has primary accountability for coordinating all response efforts.
   - Coordinate communication and information sharing between your CSIRT and internal parties, such as management and employees within your organization, and external parties, such as law enforcement, information sharing partners, hardware & software vendors, other impacted organizations, and the media. Establish points of contact with all relevant parties ahead of time and include this information in your incident response plan.
   - Create an incident response checklist that will guide your CSIRT effectively and ensure that no steps are accidentally omitted during an incident.

- Identify and acquire tools and resources to be used by your CSIRT during an incident including checklists, chain of custody forms, hardware, software, storage facilities, and evidence gathering accessories.
- Classify incidents by threat types and severity to assist in the prioritization and scope of response efforts.
- Identify the types of data your organization stores and where it is located, including key assets that may be targeted in an attack.
- Identify critical processes and develop a plan to ensure continuity during an incident.
- Establish redundant systems and back up critical data often, storing backups off the network and testing them regularly to ensure integrity and accessibility to reduce recovery times.
- Establish a network performance baseline to better identify anomalies and recognize suspicious activity during the detection & analysis phase.
- Create and include a log retention policy as part of your incident response plan.
- Audit all network user accounts to better identify unauthorized access.
- Identify and inventory all devices on your organization's network to better identify rogue and potentially malicious and unauthorized activity.
- Train all levels of staff on cybersecurity best practices, indicators of compromise (IoCs), and current cyber threats, along with how to report an incident.
- Regularly conduct tabletop exercises to ensure understanding of current procedures.

2. Detection & Analysis

- Identify precursors to, and indicators of, a cyber incident. This information can be obtained through a variety of active and passive monitoring tools such as intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) products, antivirus and antimalware software, file integrity monitoring tools, system event logs, and network device logs.
- Maintain a working knowledge of the current cyber threat landscape and awareness of current IoCs through automated indicator sharing (AIS) to quickly identify and block new and emerging threats.
- Perform event correlation across multiple logs to validate the occurrence of an incident.
- Begin documenting all data regarding an incident from the moment it is detected.
- Notify appropriate personnel of the confirmed incident as outlined in your incident response policy.

3. Containment, Eradication, & Recovery

- Isolate the impacted system(s) or device(s) from the network to prevent the threat from spreading.
- Gather and preserve evidence using sound forensic techniques. Collect identifying information of impacted systems and devices as well as all individuals who handled the evidence and where the evidence is stored.
- Remove any and all artifacts of the incident. Remove malicious code from impacted systems, sanitize compromised media, and secure compromised user accounts via password resents and implementation of multi-factor authentication.
- Perform a root cause analysis of the incident.
- Restore normal operations and adjust network and system security controls accordingly. Clean, rebuild, patch, and test affected systems, reconfigure firewall rulesets, and update malware signatures.

4. Post-Incident Activity

- Revert back to original change control processes and document any changes made during incident response.
- Conduct lessons-learned sessions for everyone involved in the response effort to highlight deficiencies in current procedures and improve response and recovery times for future incidents.
- Develop a formal after-action report that includes the chronology of events, root cause, location and description of collected evidence, specific actions taken by the CSIRT, the estimated impact on the organization and stakeholders, results of recovery efforts, and issues identified during the incident review.