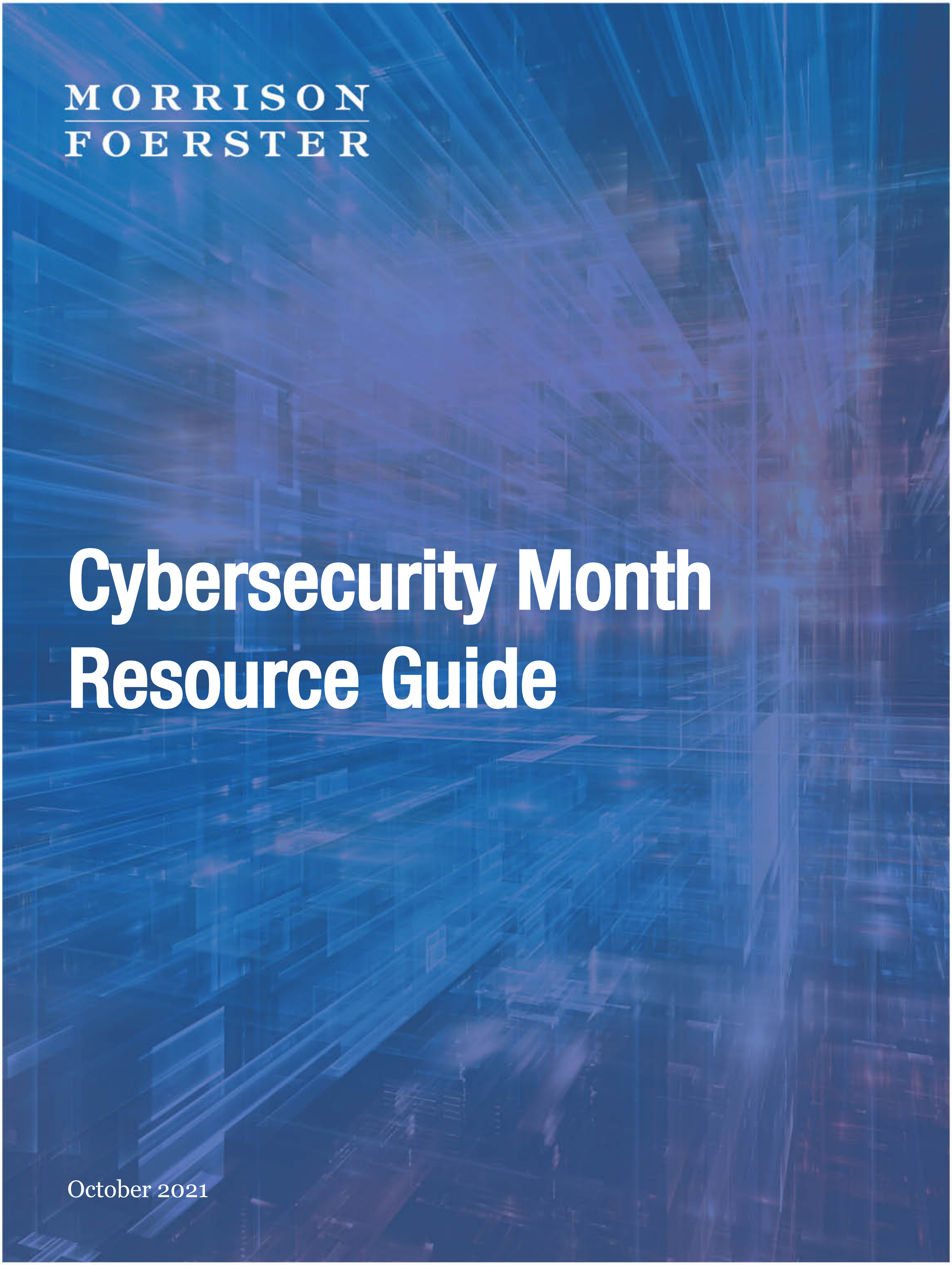


MORRISON
FOERSTER

Cybersecurity Month Resource Guide

October 2021

INSIDE

THE UNITED STATES
DEPARTMENT of JUSTICE

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Thursday, July 15, 2021

U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov

New Website Provides Cybersecurity Resources from Across the Federal Government

Today, as part of the ongoing response, agencies across the U.S. government announced new resources and initiatives to protect American businesses and communities from ransomware attacks. The U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS), together with federal partners, have launched a new website to combat the threat of ransomware. StopRansomware.gov establishes a one-stop hub for ransomware resources for individuals, businesses and other organizations. The new StopRansomware.gov is a collaborative effort across the federal government and is the first joint website created to help private and public organizations mitigate their ransomware risk.

"The Department of Justice is committed to protecting Americans from the rise in ransomware attacks that we have seen in recent years," said Attorney General Merrick B. Garland of the Justice Department. "Along with our partners in and outside of government, and through our Ransomware and Digital Extortion Task Force, the Department is working to bring all our tools to bear against these threats. But we cannot do it alone. It is critical for business leaders across industries to recognize the threat, prioritize efforts to harden their systems and work with law enforcement by reporting these attacks promptly."

"As ransomware attacks continue to rise around the world, businesses and other organizations must prioritize their cybersecurity," said Secretary Alejandro Mayorkas for the Department of Homeland Security. "Cyber criminals have targeted critical infrastructure, small businesses, hospitals, police departments, schools and more. These attacks directly impact Americans' daily lives and the security of our nation. I urge every organization across our country to use this new resource to learn how to protect themselves from ransomware and reduce their cybersecurity risk."

StopRansomware.gov is the first central hub consolidating ransomware resources from all federal government agencies. Before today, individuals and organizations had to visit a variety of websites to find guidance, latest alerts, updates and resources, increasing the likelihood of missing important information. StopRansomware.gov reduces the fragmentation of resources, which is especially detrimental for those who have become victims of an attack, by integrating federal ransomware resources into a single platform that includes clear guidance on how to report attacks, and the latest ransomware-related alerts and threats from all participating agencies. StopRansomware.gov includes resources and content from DHS's Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Secret Service, the DOJ's FBI, the Department of Commerce's National Institute of Standards and Technology (NIST), and the Departments of the Treasury and Health and Human Services.

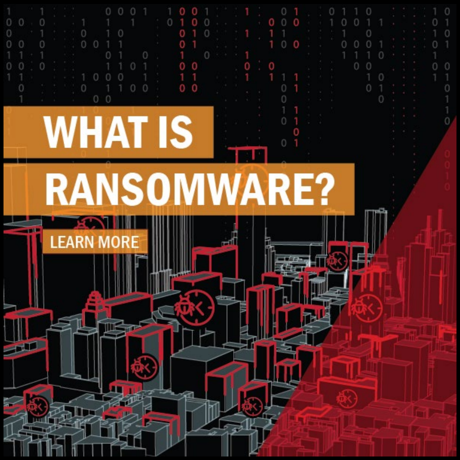
Ransomware is a long-standing problem and a growing national security threat. Tackling this challenge requires collaboration across every level of government, the private sector and our communities. Roughly $350 million in ransom was paid to malicious cyber actors in 2020, a more than 300% increase from the previous year. Further, there have already been multiple notable ransomware attacks in 2021, and despite making up roughly 75% of all ransomware cases, attacks on small businesses often go unnoticed. Like most cyber attacks, ransomware exploits the weakest link. Many small businesses have yet to adequately protect their networks, and StopRansomware.gov will help these organizations and many more to take simple steps to protect their networks and respond to ransomware incidents, while providing enterprise-level information technology (IT) teams the technical resources to reduce their ransomware risk.

DHS, DOJ, the White House and our federal partners encourage all individuals and organizations to take the frst step in protecting their cybersecurity by visiting StopRansomware.gov.

Topic(s):	Component(s):	Press Release Number:
Cyber Crime National Security	Federal Bureau of Investigation (FBI) Office of the Attorney General	21-656

An official website of the United States government Here's how you know

STOP RANSOM WARE



Protection and Response

Services

K-12 Resources

Preparation

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

HOW WE CAN HELP

General Information

FAQs

Tips

Ransomware Readiness Self-Assessment

GUIDANCE AND RESOURCES

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

READ MORE

TIPS & GUIDANCE

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small. Apply these tips and practices to avoid attack.

Good Cyber Hygiene Habits Keep Your Network Healthy

Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

When in Doubt, Report It Out

Victims of ransomware should report to federal law enforcementvia IC3 or a Secret Service Field Office, and can request technical assistance or provide information to help others by contacting CISA.

Backing Up Is Your Best Bet

Maintain offline, encrypted backups of data and regularly test your backups.

Keep Calm and Patch On

Regularly patch and update software and Operating Systems.

Learn More

REPORT AN INCIDENT

Victims of ransomware should report to federal law enforcement via IC3 or a Secret Service Field Office, and can request technical assistance or provide information to help others by contacting CISA.

REPORT

STOP RANSOMWARE

RANSOMWARE

What It Is & What To Do About It

What is Ransomware?

Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Government Efforts to Combat Ransomware

While ransomware attacks impact all sectors, the federal government is particularly concerned about the impact of ransomware on the networks of state, local, tribal, and territorial governments, municipalities, police and fire departments, hospitals, and other critical infrastructure. These types of attacks can delay a police or fire department's response to an emergency or prevent a hospital from accessing lifesaving equipment. To combat this threat, the NCIJTF has convened an interagency group of subject matter experts to educate the public on ways to prevent ransomware attacks, to improve law enforcement coordination and response, and to enable and sequence whole-of-government actions that impose consequences against the criminals engaged in this malicious activity. The Cybersecurity and Infrastructure Security Agency (CISA) leads a number of efforts including —CISA Cyber Essentials—and—CISA Insights— to assist entities in protecting themselves from cyber incidents like ransomware. More about these efforts and the tools CISA offers can be found at https://www.cisa.gov/ransomware. The FBI's IC3.gov website has additional ransomware focused resources that can be found at https://ic3.gov/Home/Ransomware.

Common Infection Vectors

Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, though recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.

- Remote Desktop Protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web market - places to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems.

- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

RANSOMWARE

What It Is & What To Do About It

Best Practices To Minimize Ransomware Risks

1. Backup your data, system images, and configurations, test your backups, and keep the backups offline
2. Utilize multi-factor authentication
3. Update and patch systems
4. Make sure your security solutions are up to date
5. Review and exercise your incident response plan

How Ransomware Has Impacted The Public Sector

The examples below may show the impacts in terms of ransom paid or service restoration cost, but it is difficult to calculate the total impact/costs of a ransomware infection. In addition, paying a ransom does not guarantee that stolen sensitive data will not be sold on the dark web.

- A U.S. county was infected by Ryuk, taking almost all of the county's systems offline. The county had backup servers, but they were not isolated from the network, allowing them to be infected as well. The county paid a $132,000 ransom.

- A U.S. city's systems were infected by Robbinhood with a ransom demand of 13 Bitcoins ($76,000). The attackers entered the network through old, out-of-date hardware and software. The ransom was not paid, but service restoration was estimated to cost over $9 million.

- A U.S. county's computer systems were infected by Ryuk. The attackers demanded over $1.2 million in Bitcoin for a decryption key. Officials decided to rebuild their systems rather than pay the ransom and spent $1 million in new equipment and technical assistance. A user allegedly opened a malicious link or attachment which caused the infection.

Reporting Information

- The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

Victims of ransomware can file a complaint with law enforcement or report incidents by:

- **Contacting your local federal law enforcement field office**
- **Filing a complaint with the Internet Crime Complaint Center (IC3)** https://ic3.gov/Home/Ransomware
- **Contacting NCIJTF CyWatch 24/7 support at 1-855-292-3937**
- **Reporting incidents, phishing, malware or vulnerabilities with CISA** https://us-cert.cisa.gov/report

IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CISA INSIGHTS

DEFEND TODAY,
SECURE TOMORROW

JANUARY 2021

Cybersecurity Perspectives:
Healthcare and Public Health Response to COVID-19

THREATS TO THE HEALTHCARE AND PUBLIC HEALTH (HPH) SECTOR

Disruptive ransomware and other malicious cyber attacks significantly reduce HPH entities' ability to provide patient care and can contribute to patient mortality. Threat actors aim to disrupt HPH entities who have a low tolerance for down-time and may be experiencing resource and staffing constraints due to the COVID-19 pandemic.

CISA recommends that all HPH entities review the following observations and findings, which are derived from an analysis of HPH entities enrolled in CISA's free vulnerability scanning service from March to October 2020, and take appropriate action to reduce potential vulnerability and maintain resilient cybersecurity practices. Email **vulnerability_info@cisa.dhs.gov** to sign up for free **CISA Cyber Hygiene Services**.

CONCERNS	Threat actors are leveraging internet-facing risky ports and services (e.g. RDP) to establish initial access to networks and deliver ransomware	Cyber threat actors are chaining critical vulnerabilities on perimeter devices with newer vulnerabilities to compromise networks and escalate	Unsupported software and operating systems (OS) are being used on internet-facing assets, leaving systems vulnerable to widely known exploits
FINDINGS MAR TO OCT 2020	**49%** of enrolled HPH entities had risky ports and services exposed on internet-facing assets	Recent chaining attacks are exploiting unpatched Virtual Private Network (VPN) and perimeter device vulnerabilities	**58%** of enrolled HPH entities were using unsupported legacy or end-of-life software and OS
TARGETED MITIGATIONS	**Restrict internet-facing risky services** • Limit exposure by disabling or securely configuring (e.g. enable multi-factor authentication and encryption risky services such as: — RDP — SMB — Telnet — DICOM • Perform cost-benefit analysis of existing risky services exposed to the internet	**Maintain diligent mission critical patching** • Patch actively exploited vulnerabilities first • Review vulnerability backlogs and patch legacy CVEs that may be used in chaining attacks • Triage then apply patches and software updates on systems supporting hospital operations and patient care • Implement compensating controls or adjust security architecture to mitigate risk when patching is not possible	**Secure/retire legacy systems** • Isolate and segment legacy systems to prevent lateral movement • Upgrade or replace unsupported legacy software and OS • Maintain accurate hardware and software inventory

BASELINE PREPARATION FOR LIKELY ATTACKS

- Maintain backups in secure offline environments and regularly test backups
- Filter emails with known malicious indicators at the email gateway
- Monitor network for malcious activity and signs of attack
- Focus phishing training on current events and reporting suspicious activity
- Implement and test cyber incident response plans

ADDITIONAL RESOURCES

- CISA and MS-ISAC **Joint Ransomware Guide** and CISA, FBI, and HHS Joint **HPH Cybersecurity Advisory**
- Health Sector Coordinating Council (HSCC) and HHS **Health Industry Cybersecurity Practices**
- **Health Sector Cybersecurity Coordination Center (HC3)** and **Health Information Sharing and Analysis Center (H-ISAC)**

PLEASE SHARE YOUR THOUGHTS. WE RECENTLY UPDATED OUR ANONYMOUS **PRODUCT SURVEY**; WE'D WELCOME YOUR FEEDBACK.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

This advisory describes the potential sanctions risks associated with making and facilitating ransomware payments and provides information for contacting relevant U.S. government agencies, including OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[3]

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a

[1] This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive, or as imposing requirements under U.S. law, or otherwise addressing any requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

[2] This advisory updates and supersedes OFAC's *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* of October 1, 2020.

[3] This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

ransomware payment, usually through virtual currency, in exchange for a key to decrypt the files and restore victims' access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation (FBI), there was a nearly 21 percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020.[4] Ransomware attacks are carried out against private and governmental entities of all sizes and in all sectors, including organizations operating critical infrastructure, such as hospitals. Often attacks also take place against vulnerable entities such as school districts and smaller businesses, in part due to the attacker's assumption that such victims may have fewer resources to invest in cyber protection and will make quick payment to restore services.

OFAC Designations of Malicious Cyber Actors

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States.[5] OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.[6]

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two virtual currency addresses used to funnel SamSam ransomware proceeds.[7]

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two sub-groups, Bluenoroff and Andariel, in September 2019.[8]

[4] *Compare* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf, *with* Federal Bureau of Investigation, Internet Crime Complaint Center, *2020 Internet Crime Report*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[5] Press Release, U.S. Dept. of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), available at https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

[6] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), available at https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx.

[7] Press Release, U.S. Dept. of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.

[8] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), available at https://home.treasury.gov/news/press-releases/sm774.

Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.[9]

In September 2021, OFAC designated SUEX OTC, S.R.O. ("SUEX"), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors, involving illicit proceeds from at least eight ransomware variants. Analysis of known SUEX transactions showed that over 40% of SUEX's known transaction history was associated with illicit actors.[10]

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.[11]

<u>Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests</u>

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks. Moreover, there is no guarantee that companies will regain access to their data or be free from further attacks themselves. For these reasons, the U.S. government strongly discourages the payment of cyber ransom or extortion demands.

<u>Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations</u>

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[12] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of

[9] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), available at https://home.treasury.gov/news/press-releases/sm845.

[10] Press Release, U.S. Dept. of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), available at https://home.treasury.gov/news/press-releases/jy0364.

[11] Federal charges have also been brought in connection with each of the aforementioned ransomware schemes. *See*, e.g., Press Release, U.S. Dept. of Justice, Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware (Dec. 5, 2019), available at https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens; and Press Release U.S. Dept. of Justice, Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe (Feb. 17, 2021), available at https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and#:~:text=A%20federal%20indictment%20unsealed%20today,and%20companies%2C%20to%20create%20.

[12] 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including a transaction by a non-U.S. person that causes a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations.

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC's Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)[13] provide more information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Enforcement responses range from non-public responses, including issuing a No Action Letter or a Cautionary Letter, to public responses, such as civil monetary penalties.

Sanctions Compliance Program and Defensive/Resilience Measures

Under OFAC's Enforcement Guidelines, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response to an apparent violation of U.S. sanctions laws or regulations.

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.[14] This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.[15]

Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide,[16] will be

[13] 31 C.F.R. part 501, appx. A.

[14] To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The *Framework* is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

[15] *See* FinCEN Guidance, FIN-2020-A006, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.

[16] *See* Cybersecurity and Infrastructure Security Agency Guidance, *Ransomware Guide*, September 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.

considered a significant mitigating factor in any OFAC enforcement response.[17] Such steps could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others.

Cooperation with OFAC and Law Enforcement

Another factor that OFAC will consider under the Enforcement Guidelines is the reporting of ransomware attacks to appropriate U.S. government agencies and the nature and extent of a subject person's cooperation with OFAC, law enforcement, and other relevant agencies, including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed. In the case of ransomware payments that may have a sanctions nexus, OFAC will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA or the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response. OFAC will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor.

While the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took the mitigating steps described above, particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will continue to be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible. Victims should also report ransomware attacks and payments to Treasury's OCCIP and contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment. As noted, in doing so victims can receive significant mitigation from OFAC when determining an appropriate enforcement response in the event a sanctions nexus is found in connection with a ransomware payment.

[17] *See* the U.S. government's website, https://www.cisa.gov/stopransomware, for additional guidance.

By reporting ransomware attacks as soon as possible, victims may also increase the likelihood of recovering access to their data through other means, such as alternative decryption tools, and in some circumstances may be able to recover some of the ransomware payment. Additionally, reporting ransomware attacks and payments provides critical information needed to track cyber actors, hold them accountable, and prevent or disrupt future attacks.

Contact Information for U.S. Department of Treasury Agencies:

- U.S. Department of the Treasury's Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)
  - FinCEN Regulatory Support Section: frc@fincen.gov

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
  - https://www.ic3.gov/default.aspx; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
  - https://secretservice.gov/contact/field-offices
- Cybersecurity and Infrastructure Security Agency
  - https://us-cert.cisa.gov/forms/report
- Homeland Security Investigations Field Office
  - https://www.ice.gov/contact/hsi

Ransomware Prevention Resources:

- U.S. Government StopRansomWare.gov Website
  - https://www.cisa.gov/stopransomware
- CISA Ransomware Guide
  - https://www.cisa.gov/stopransomware/ransomware-guide

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.

RANSOMWARE GUIDE

SEPTEMBER 2020

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Overview

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

This *Ransomware Guide* includes two resources:
Part 1: Ransomware Prevention Best Practices
Part 2: Ransomware Response Checklist

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - □ Multi-State Information Sharing and Analysis Center (MS-ISAC): **https://learn.cisecurity.org/ms-isac-registration**
  - □ Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): **https://learn.cisecurity.org/ei-isac-registration**
  - □ Sector-based ISACs - National Council of ISACs: **https://www.nationalisacs.org/member-isacs**
  - □ Information Sharing and Analysis Organization (ISAO) Standards Organization: **https://www.isao.org/information-sharing-groups/**
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more.
  - □ SLTT organizations: **CyberLiaison_SLTT@cisa.dhs.gov**
  - □ Private sector organizations: **CyberLiaison_Industry@cisa.dhs.gov**

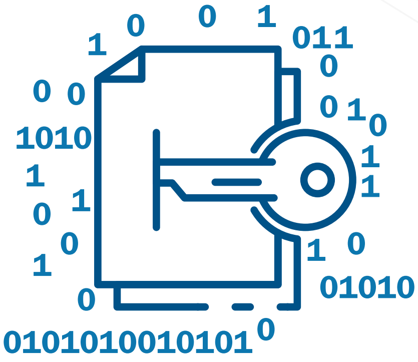
Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as the *Public Power Cyber Incident Response Playbook* (**https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf**), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - The Ransomware Response Checklist, which forms the other half of this *Ransomware Guide*, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.



Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
    - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.
- Regularly patch and update software and OSs to the latest available versions.
    - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (**https://us-cert.cisa.gov/ncas/alerts/aa20-073a**).
    - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:
    - Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.
        - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
    - Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both "precursor" malware and ransomware.
    - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
    - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
    - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
    - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.

For more information on DMARC, see: **https://www.cisecurity.org/blog/how-dmarc-advances-email-security/** and

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C.pdf.

Funded by CISA, the MS-ISAC and EI-ISAC provide the Malicious Domain Blocking and Reporting (MDBR) service at no-cost to members. MDBR is a fully managed proactive security service that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known malware, ransomware, phishing, and other cyber threats. To sign up for MDBR, visit: **https://www.cisecurity.org/ms-isac/services/mdbr/.**

CISA and MS-ISAC encourage SLTT organizations to consider the Albert IDS to enhance a defense-in-depth strategy. CISA funds Albert sensors deployed by the MS-ISAC, and we encourage SLTT governments to make use of them. Albert serves as an early warning capability for the Nation's SLTT governments and supports the nationwide cybersecurity situational awareness of CISA and the Federal Government. For more information regarding Albert, see: **https://www.cisecurity.org/services/albert-network-monitoring/.**

Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
    - If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA's APTs Targeting IT Service Provider Customers (**https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers**).
    - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.
    - Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
    - If you are using passwords, use strong passwords (**https://us-cert.cisa.gov/ncas/tips/ST04-002**) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
    - Restrict user permissions to install and run software applications.
    - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.

    - Remove unnecessary accounts and groups and restrict root access.
    - Control and limit local administration.
    - Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
    - Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.
- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (**https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a**).
- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
    - The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.

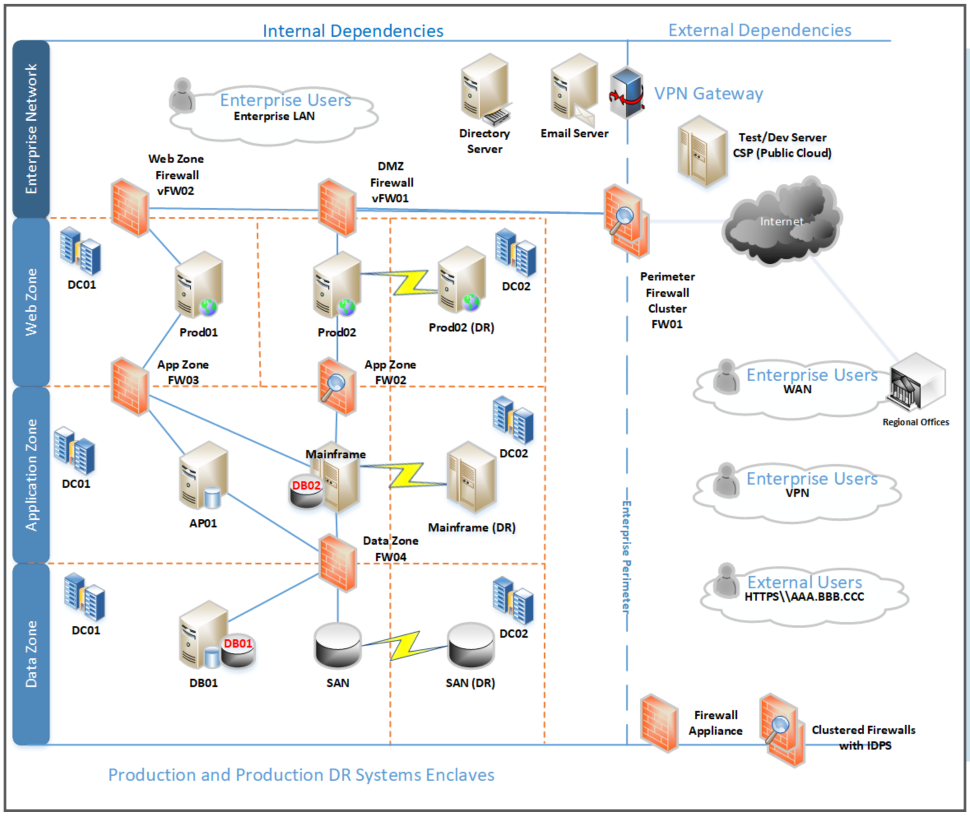


Figure 1. Example Network Diagram

This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.

  - Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).

- Ensure your organization has a comprehensive asset management approach.
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
  - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
  - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: **https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/**.
- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
  - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
  - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).

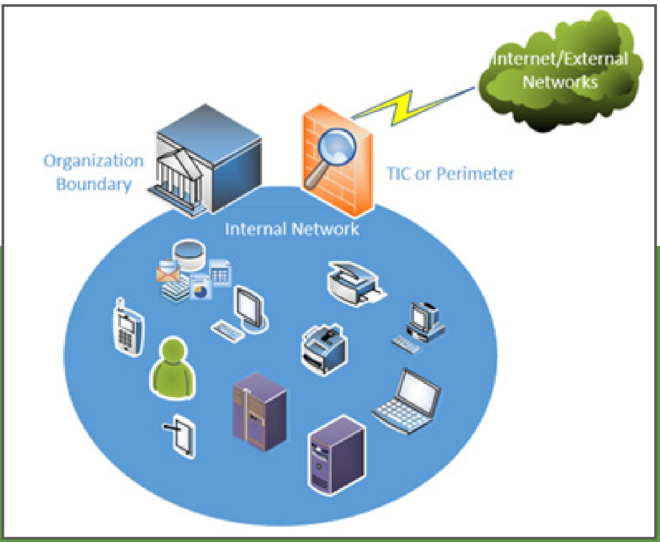


Figure 2. Flat (Unsegmented) Network

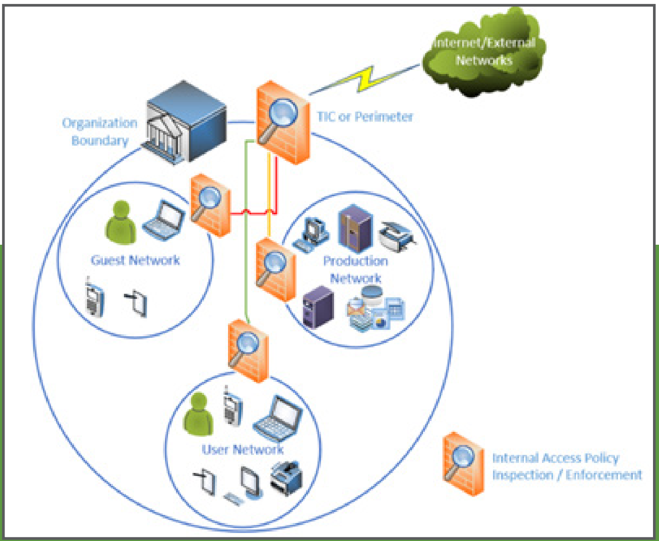


Figure 3. Segmented Network

        - The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
    - The following list contains high-level suggestions on how best to secure a DC:
        - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
        - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (**https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory**), when configuring available security features.
        - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
        - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
        - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
    - CISA recommends the following DC Group Policy settings:

      (Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
        - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
        - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.
        - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.
- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.

- □ Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
- □ Maintain and back up logs for critical systems for a minimum of one year, if possible.

- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
  - □ Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.

Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve their defenses to avoid ransomware infection: **https://www.cisa.gov/cyber-resource-hub**
  - □ Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- **Cyber exercises** evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- **CISA Cybersecurity Advisors (CSAs)** advise on best practices and connect you with CISA resources to manage cyber risk
- **Contacts:**
  - □ **SLTT organizations:** **CyberLiaison_SLTT@cisa.dhs.gov**
  - □ **Private sector organizations:** **CyberLiaison_Industry@cisa.dhs.gov**

Ransomware Quick References

- **Ransomware: What It Is and What to Do About It (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: **https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf**
- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: **https://www.us-cert.cisa.gov/Ransomware**
- **Security Primer – Ransomware (MS-ISAC):** Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: **https://www.cisecurity.org/white-papers/security-primer-ransomware/**
- **Ransomware: Facts, Threats, and Countermeasures (MS-ISAC):** Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: **https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/**
- **Security Primer – Ryuk (MS-ISAC):** Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: **https://www.cisecurity.org/white-papers/security-primer-ryuk/**

Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Detection and Analysis

☐ 1. Determine which systems were impacted, and immediately isolate them.

- ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- ☐ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

☐ 2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

☐ 3. Triage impacted systems for restoration and recovery.

- ☐ Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.
  - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ 4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.

☐ 5. Using the contact information below, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

- ☐ Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.

If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

□ Recovered executable file

□ Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible

□ Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)

□ Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)

□ Malware samples

□ Names of any other malware identified on your system

□ Encrypted file samples

□ Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)

□ Any PowerShell scripts found having executed on the systems

□ Any user accounts created in Active Directory or machines added to the network during the exploitation

□ Email addresses used by the attackers and any associated phishing emails

□ A copy of the ransom note

□ Ransom amount and whether or not the ransom was paid

□ Bitcoin wallets used by the attackers

□ Bitcoin wallets used to pay the ransom (if applicable)

□ Copies of any communications with attackers

Remember: Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and federal law enforcement do not recommend paying ransom.

□ Consider requesting assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS]). See contact information below.

□ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.

□ The *Public Power Cyber Incident Response Playbook* (**https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf**) contains guidance for organizational communication procedures as well as templates for cyber incident holding statements for public consumption. Work with your team to develop similar procedures and draft holding statements as soon as possible, as developing this documentation during an incident is not optimal. This will allow your organization to reach consensus, in advance, on what level of detail is appropriate to share within the organization and with the public, and how information will flow.

Containment and Eradication

If no initial mitigation actions appear possible:

□ 6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.

□ Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

□ 7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

To continue taking steps to contain and mitigate the incident:

□ 8. Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

- □ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known, associated registry values and files.

□ 9. Identify the systems and accounts involved in the initial breach. This can include email accounts.

□ 10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:

- □ Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

□ 11. Additional suggested actions—server-side data encryption quick-identification steps:

- □ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:

  1. Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.

  2. Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.

  3. Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.

  4. Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events.

  5. Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., "smb2.filename contains cryptxxx").

□ 12. Conduct an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

Upon voluntary request, CISA and MS-ISAC can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested:

- ■ CISA – Advanced Malware Analysis Center: **https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf**
- ■ MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): **https://www.cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/**
  - □ Scans a suspicious file or Uniform Resource Locator (URL) against several antivirus vendors to determine if it matches known malicious signatures
  - □ Runs a file or URL in a sandbox to analyze behavior
  - □ Provides a user with a summary report of malware behavior, including files accessed, tasks created, outbound connections, and other behavioral traits
  - □ Users can opt to keep submissions private and make direct requests for assistance from MS-ISAC; users can also mark submissions for sharing with CISA
  - □ Email: **mcap@cisecurity.org** to set up an account
- ■ Remote Assistance – Request via CISA Central or MS-ISAC Security Operations Center (see contact information below)

- □ Look for evidence of precursor “dropper” malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex, or Emotet.
  - Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network in an attempt to further extort the victim and pressure them into paying.
  - Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.

☐ 13. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.

- □ Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
- □ Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
- □ Identification may involve deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

☐ 14. Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), using pre-configured standard images, if possible.

☐ 15. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.

☐ 16. Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.

Recovery and Post-Incident Activity

☐ 17. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.

- □ Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.

☐ 18. Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.

☐ 19. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community.

Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:

Contact	24x7 Contact Information	Roles and Responsibilities
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Federal Asset Response Contacts

Upon voluntary request, federal asset response includes providing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk, assessing potential risks to the sector or region, facilitating information sharing and operational coordination, and providing guidance on how to best use federal resources and capabilities.

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant)
- Phishing email, storage media, log and malware analysis, based on voluntary submission (full-disk forensics can be performed on an as-needed basis)
- Contacts:
  - □ CISA:
    - **https://us-cert.cisa.gov/report**, **Central@cisa.gov** or (888) 282-0870
    - Cybersecurity Advisor (**https://www.cisa.gov/cisa-regions**): [Enter your local CISA CSA's phone number and email address.]
  - □ MS-ISAC:
    - **soc@msisac.org** or (866) 787-4722

Federal Threat Response Contacts

Upon voluntary request, federal threat response includes law enforcement and national security investigative activity: collecting evidence and intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

What You Can Expect:

- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
- Contacts:
  - □ FBI:
    - **https://www.fbi.gov/contact-us/field-offices**
    - [Enter your local FBI field office POC phone number and email address.]
  - □ USSS:
    - **https://www.secretservice.gov/contact/field-offices/**
    - [Enter your local USSS field office POC phone number and email address.]

DEFEND TODAY,

SECURE TOMORROW

CISA.GOV

MS-ISAC®

Multi-State Information Sharing & Analysis Center®

Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229 and 249

[Release Nos. 33-10459; 34-82746]

Commission Statement and Guidance on Public Company Cybersecurity Disclosures

AGENCY: Securities and Exchange Commission.

ACTION: Interpretation.

SUMMARY: The Securities and Exchange Commission (the "Commission") is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

DATES: Applicable: February 26, 2018

FOR FURTHER INFORMATION CONTACT: Questions about specific filings should be directed to staff members responsible for reviewing the documents the company files with the Commission. For general questions about this release, contact the Office of the Chief Counsel at (202) 551-3500 in the Division of Corporation Finance, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION:

I. Introduction

A. Cybersecurity

Cybersecurity risks pose grave threats to investors, our capital markets, and our country.[1]

[1] The U.S. Computer Emergency Readiness Team defines cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#C (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May

Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks. Companies today rely on digital technology to conduct their business operations and engage with their customers, business partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.

As companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased.[2] Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century. Cybersecurity incidents[3] can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and "hacktivists."[4] Companies face an evolving

2009).

[2] See World Economic Forum, Global Risks Report 2017, 12th Ed. (Jan. 2017), available at https://www.weforum.org/reports/the-global-risks-report-2017 (concluding that "greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyber-attacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways."). See also PwC, "Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016" (Oct. 2015), available at https://www.pwccn.com/en/retail-and-consumer/rcs-info-security-2016.pdf. (finding that in 2015 there was a reported 38% increase in detected information security incidents from 2014).

[3] A "cybersecurity incident" is "[a]n occurrence that actually or potentially results in adverse consequences to … an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#I.

[4] One study using a sample of 419 companies in 13 countries and regions noted that 47 percent of data breach incidents in 2016 involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures. See

landscape of cybersecurity threats in which hackers use a complex array of means to perpetrate cyber-attacks, including the use of stolen access credentials, malware, ransomware, phishing, structured query language injection attacks, and distributed denial-of-service attacks, among other means. The objectives of cyber-attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners. Cyber-attacks may also be directed at disrupting the operations of public companies or their business partners. This includes targeting companies that operate in industries responsible for critical infrastructure.

Companies that fall victim to successful cyber-attacks or experience other cybersecurity incidents may incur substantial costs[5] and suffer other negative consequences, which may include:

- remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;[6]
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;

Ponemon Institute and IBM Security, 2017 Cost of Data Breach Study: Global Overview (Jun. 2017), available at https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.

[5] The average organizational cost of a data breach in the United States in 2016 was $7.35 million based on the sample in the study. Id. However, the total costs a company may incur in connection with a particular cyber-attack or incident could be much higher.

[6] A company's costs may also include payments to perpetrators of ransomware attacks in order to attempt to restore operations or protect customer data or other proprietary information. But see Federal Bureau of Investigation, "How To Protect your Network from Ransomware," Ransomware Prevention and Response for CISOs, available at https://www.justice.gov/criminal-ccips/file/872771/download.

- lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;[7]
- increased insurance premiums;
- reputational damage that adversely affects customer or investor confidence; and
- damage to the company's competitiveness, stock price, and long-term shareholder value.

Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack. Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.[8] In addition, the Commission believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has

[7] See, e.g., New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies; European Union General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 1.

[8] See Section II.B.1 below for further discussion of disclosure controls and procedures.

faced or is likely to face.

Additionally, directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company. Public companies should have policies and procedures in place to (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information.[9] In addition, we believe that companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material. We recognize that many companies have adopted preventative measures to address the appearance of improper trading and we encourage companies to consider such preventative measures in the context of a cyber event.

B. CF Disclosure Guidance: Topic No. 2

In October 2011, the Division of Corporation Finance (the "Division") issued guidance that provided the Division's views regarding disclosure obligations relating to cybersecurity risks and incidents.[10] The guidance explains that, although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be

[9] See Section II.B.2 below for further discussion of insider trading.

[10] See CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

obligated to disclose such risks and incidents.[11] After the issuance of the guidance, many companies included additional cybersecurity disclosure, typically in the form of risk factors.[12]

C. Purpose of Release

In light of the increasing significance of cybersecurity incidents, the Commission believes it is necessary to provide further Commission guidance. This interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies.[13] While the Commission continues to consider other means of promoting appropriate disclosure of cyber incidents, we are reinforcing and expanding upon the staff's 2011 guidance. In addition, we address two topics not developed in the staff's 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make

[11] Id.

[12] For example, Willis North America released a 2013 report that found that approximately 88% of the public Fortune 500 companies and about 78% of the Fortune 501-1000 companies included risk factor disclosure regarding cybersecurity in their annual reports filed in 2012. See Willis Fortune 1000 Cyber Disclosure Report (Aug. 2013), available at http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf. In 2015, over 88% of Russell 3000 companies disclosed cybersecurity as a risk. See Audit Analytics, "Cybersecurity Disclosure in Risk Factors," (Jan. 14, 2016), available at http://www.auditanalytics.com/blog/cybersecurity-disclosures-in-risk-factors/.

[13] This release does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations. For example, in 2014 the Commission adopted Regulation Systems Compliance and Integrity, applicable to certain self-regulatory organizations, to strengthen the technology infrastructure of the U.S. securities markets. Final Rule: Regulation Systems Compliance and Integrity, Release No. 34-73639 (Nov. 19, 2014) [79 FR. 72252 (Dec. 5, 2014)], available at https://www.sec.gov/rules/final/2014/34-73639.pdf. For additional cybersecurity regulations and resources, see the Commission's website page devoted to cybersecurity issues, available at https://www.sec.gov/spotlight/cybersecurity; see also Cybersecurity Guidance; IM Guidance Update (April 2015), available at https://www.sec.gov/investment/im-guidance-2015-02.pdf (staff guidance on cybersecurity measures for registered investment companies and investment advisers).

accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws.

Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.[14]

The Commission, and the staff through its filing review process, continues to monitor cybersecurity disclosures carefully.

II. Commission Guidance

A. Overview of Rules Requiring Disclosure of Cybersecurity Issues

1. Disclosure Obligations Generally; Materiality

Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"), and periodic and current reports under the Exchange Act.[15] When a company is required to file a disclosure

[14] See Final Rule: Selective Disclosure and Insider Trading, Release No. 33-7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)], available at https://www.sec.gov/rules/final/33-7881.htm.

[15] Listed companies also should consider any obligations that may be imposed by exchange listing requirements. For example, the NYSE requires listed companies to "release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities." See NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments. In addition, in 2015, the NYSE, in partnership with Palo Alto Networks, published a summary of information about legal and regulatory aspects of cybersecurity governance for directors and officers of public companies. See Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc., 2015, available at https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf. Similarly, Nasdaq requires listed companies to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions." See Nasdaq Listing Rule 5250(b)(1).

document with the Commission, the requisite form generally refers to the disclosure requirements of Regulation S-K[16] and Regulation S-X.[17] Although these disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to disclose such risks and incidents depending on a company's particular circumstances. For example:

- Periodic Reports: Companies are required to file periodic reports[18] to disclose specified information on a regular and ongoing basis.[19] These periodic reports include annual reports on Form 10-K,[20] which require companies to make disclosure regarding their business and operations, risk factors, legal proceedings, management's discussion and analysis of financial condition and results of operations ("MD&A"), financial statements, disclosure controls and procedures, and corporate governance.[21] Periodic reports also include quarterly reports on Form 10-Q,[22] which require companies to make disclosure regarding their

[16] 17 CFR part 229.

[17] 17 CFR part 210.

[18] An issuer with a class of securities registered under Section 12 or subject to Section 15(d) of the Exchange Act is subject to the periodic and current reporting requirements of Section 13 and 15(d), respectively, of the Exchange Act.

[19] "Congress recognized that the ongoing dissemination of accurate information by companies about themselves and their securities is essential to effective operation of the trading markets. The Exchange Act rules require public companies to make periodic disclosures at annual and quarterly intervals, with other important information reported on a more current basis. The Exchange Act specifically provides for current disclosure to maintain the currency and adequacy of information disclosed by companies." Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, Release No. 33-8106, 3-4 (Jun. 17, 2002) [67 FR 42914 (Jun. 25, 2002)].

[20] 17 CFR 249.310.

[21] See Part I, Items 1, 1A and 3 of Form 10-K; Part II, Items 7, 8 and 9A of Form 10-K; and Part III, Item 10 of Form 10-K [17 CFR 249.310].

[22] 17 CFR 249.308a.

financial statements, MD&A, and updated risk factors.[23] Likewise, foreign private issuers are required to make many of these same disclosures in their periodic reports on Form 20-F.[24] Companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.

- Securities Act and Exchange Act Obligations: Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.[25]
- Current Reports: In order to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents,[26] companies can provide current reports on Form 8-K[27] or Form 6-K.[28] Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity

[23] See Part I, Items 1 and 2 of Form 10-Q; Part II, Item 1A of Form 10-Q [17 CFR 249.308a].

[24] See Part I, Items 3.D, 4, 5 and 8 of Form 20-F; Part II, Items 15 and 16G of Form 20-F; Part III, Items 17 and 18 of Form 20-F [17 CFR 249.220f].

[25] 15 U.S.C. 77k; 15 U.S.C. 77l; 15 U.S.C. 77q; 15 U.S.C 78j(b); 17 CFR 240.10b-5.

[26] See Item 11(a) of Form S-3 [17 CFR 239.13] and Item 5(a) of Form F-3 [17 CFR 239.33].

[27] 17 CFR 249.308.

[28] 17 CFR 249.306.

> incidents.[29] The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur.[30]

In addition to the information expressly required by Commission regulation, a company is required to disclose “such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading.”[31] The Commission considers omitted information to be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available.[32]

In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact

[29] “The registrant may, at its option, disclose under this Item 8.01 [of Form 8-K] any events, with respect to which information is not otherwise called for by this form, that the registrant deems of importance to security holders.” 17 CFR 308.

[30] See Sections II.B.2 and II.B.3 below for further discussion of insider trading and Regulation FD.

[31] Rule 408 of the Securities Act [17 CFR 230.408]; Rule 12b-20 of the Exchange Act [17 CFR 240.12b-20]; and Rule 14a-9 of the Exchange Act [17 CFR 240.14a-9].

[32] This approach is consistent with the standard of materiality articulated by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (a fact is material “if there is a substantial likelihood that a reasonable shareholder would consider it important” in making an investment decision or if it “would have been viewed by the reasonable investor as having significantly altered the ‘total mix’ of information made available” to the shareholder).

of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations.[33] The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause.[34] This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts – for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale

[33] For example, the compromised information might include personally identifiable information, trade secrets or other confidential business information, the materiality of which may depend on the nature of the company's business, as well as the scope of the compromised information.

[34] As part of a materiality analysis, a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity. Basic v. Levinson, 485 U.S. 224, 238 (1988) (citing SEC v. Texas Gulf Sulphur Co., 401 F. 2d 833, 849 (2d Cir. 1968)). Moreover, no "single fact or occurrence" is determinative as to materiality, which requires an inherently fact-specific inquiry. Basic, 485 U.S. at 236.

of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.[35]

Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

We remind companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made[36] (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made[37] (for example, when the original statement is still being relied on by reasonable investors). Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

[35] See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15. U.S.C. 78o(d); 17 CFR 240.10b-5].

[36] See Backman v. Polaroid Corp., 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies "if a disclosure is in fact misleading when made, and the speaker thereafter learns of this.").

[37] See id. at 17 (describing the duty to update as potentially applying "if a prior disclosure 'becomes materially misleading in light of subsequent events'" (quoting Greenfield v. Heublein, Inc., 742 F.2d 751, 758 (3d Cir. 1984))). But see Higginbotham v. Baxter Intern., Inc., 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); Gallagher v. Abbott Laboratories, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).

We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we "emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies."[38] Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

2. Risk Factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company's securities speculative or risky.[39] Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.[40]

It would be helpful for companies to consider the following issues, among others, in evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;

[38] See Business and Financial Disclosure Required by Regulation S-K, Release No. 33-10064 (Apr. 13, 2016) [81 FR 23915 (Apr. 22, 2016)]. See also Plain English Disclosure, Release No. 33-7497 (Jan. 28, 1998) [63 FR 6370 (Feb. 6, 1998)]; and Updated Staff Legal Bulletin No. 7: Plain English Disclosure (Jun. 7, 1999) available at https://www.sec.gov/interps/legal/cfslb7a.htm.

[39] 17 CFR 229.503(c); 17 CFR 249.220f.

[40] See Final Rule: Business Combination Transactions, Release No. 33-6578 (Apr. 23, 1985) [50 FR 18990 (May 6, 1985)].

- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

3. MD&A of Financial Condition and Results of Operations

Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations.[41] In this context, the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation,

[41] 17 CFR 229.303; 17 CFR 249.220f.

and the loss of competitive advantage that may result.[42] Finally, the Commission expects companies to consider the impact of such incidents on each of their reportable segments.[43]

4. Description of Business

Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions.[44] If cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure.

5. Legal Proceedings

Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party.[45] Companies should note that this requirement includes any such proceedings that relate to cybersecurity issues. For example, if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

[42] A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056 (Dec. 29, 2003)]; Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746 (Jan. 25, 2002)]; Management's Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427 (May 24, 1989)].

[43] 17 CFR 229.303(a).

[44] 17 CFR 229.101; 17 CFR 249.220f.

[45] 17 CFR 229.103.

6. Financial Statement Disclosures

Cybersecurity incidents and the risks that result therefrom may affect a company's financial statements. For example, cybersecurity incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
- loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases; and
- diminished future cash flows, impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

The Commission expects that a company's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.[46]

7. Board Risk Oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[47] The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to

[46] See Section 13(b)(2)(B) of the Exchange Act [15 U.S.C.78m(b)(2)(B)].

[47] 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.

investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[48] A company must include a description of how the board administers its risk oversight function.[49] To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk.

In addition, we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

B. Policies and Procedures

1. Disclosure Controls and Procedures

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and

[48] Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (Dec. 16, 2009) [74 FR 68334 (Dec. 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.

[49] See Item 407(h) of Regulation S-K [17 CFR 229.407(h)].

other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.[50]

Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness.[51] These rules define "disclosure controls and procedures" as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) "recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms," and (2) "accumulated and communicated to the company's management … as appropriate to allow timely decisions regarding required disclosure."[52]

A company's disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses.[53] Information also must be

[50] See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that, to assist principal executive and financial officers in the discharge of their responsibilities in making the required certifications, as well as to discharge their responsibilities in providing accurate and complete information to security holders, it is necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner."); see also Section 10(b) of the Exchange Act and Rule 10b-5 thereunder [15 U.S.C. 78j(b); 17 CFR 240.10b-5].

[51] 17 CFR 240.13a-15; 17 CFR 240.15d-15.

[52] Id.

[53] See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that the new rules will help to ensure that an issuer's systems grow and evolve with its business and are capable of producing Exchange Act reports that are timely, accurate and reliable.").

evaluated in the context of the disclosure requirement of Exchange Act Rule 12b-20.[54] When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

Exchange Act Rules 13a-14 and 15d-14[55] require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures,[56] and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures.[57] These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

[54] 17 CFR 240.12b-20.

[55] 17 CFR 240.13a-14; 17 CFR 240.15d-14.

[56] Section 302 of the Sarbanes-Oxley Act of 2002 required the Commission to adopt final rules under which the principal executive officer or officers and the principal financial officer or officers, or persons providing similar functions, of an issuer each must certify the information contained in the issuer's quarterly and annual reports. Pub. L. 107-204, 116 Stat. 745 (2002).

[57] 17 CFR 229.307; 17 CFR 249.220f.

2. Insider Trading

Companies and their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches.[58] It is illegal to trade a security "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information."[59] As noted above, information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.[60]

Beyond the antifraud provisions of the federal securities laws, companies and their directors, officers, and other corporate insiders must comply with all other applicable insider trading related rules. Many exchanges require listed companies to adopt codes of conduct and policies that promote compliance with applicable laws, rules, and regulations, including those prohibiting insider trading.[61] We encourage companies to consider how their codes of ethics[62]

[58] In addition to promoting full and fair disclosure, the antifraud provisions of the federal securities laws prohibit insider trading, which harms not only individual investors but also the very foundations of our markets by undermining investor confidence in the integrity of those markets. 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

[59] Rule 10b5-1(a) of the Exchange Act [17 CFR 240.10b-5-1(a)].

[60] This would not preclude directors, officers, and other corporate insiders from relying on Exchange Act Rule 10b5-1 if all conditions of that rule are met.

[61] See e.g., NYSE Listed Company Manual Section 303A.10, which states in relevant part that every NYSE "listed company should proactively promote compliance with laws, rules and regulations, including insider trading laws.

and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. The Commission believes that it is important to have well designed policies and procedures to prevent trading on the basis of all types of material non-public information, including information relating to cybersecurity risks and incidents.

In addition, while companies are investigating and assessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents, they should consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. Company insider trading policies and procedures that include prophylactic measures can protect against directors, officers, and other corporate insiders trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident. As noted above, we believe that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.

3. Regulation FD and Selective Disclosure

Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Under Regulation FD, "when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information."[63] The Commission adopted Regulation FD owing to concerns

Insider trading is both unethical and illegal, and should be dealt with decisively." See also NASDAQ Listing Rule 5610 and Section 406(c) of the Sarbanes-Oxley Act of 2002.

[62] Item 406 of Regulation S-K [17 CFR 229.406].

[63] 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

about companies making selective disclosure of material nonpublic information to certain persons before making full disclosure of that same information to the general public.[64]

In cases of selective disclosure of material nonpublic information related to cybersecurity, companies should ensure compliance with Regulation FD. Companies and persons acting on their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons[65] before disclosing that same information to the public.[66] We expect companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to

[64] Id.

[65] Regulation FD applies generally to selective disclosures made to persons outside the issuer who are (1) a broker or dealer or persons associated with a broker or dealer; (2) an investment advisor or persons associated with an investment advisor; (3) an investment company or persons affiliated with an investment company; or (4) a holder of the issuer's securities under circumstances in which it is reasonably foreseeable that the person will trade in the issuer's securities on the basis of the information. 17 CFR 243.100(b)(1).

[66] Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made simultaneously (in the case of an intentional disclosure as defined in the rule) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation.[67]

By the Commission.

Dated: February 21, 2018

Brent J. Fields
Secretary

[67] "Under the regulation, the required public disclosure may be made by filing or furnishing a Form 8-K, or by another method or combination of methods that is reasonably designed to effect broad, non-exclusionary distribution of the information to the public." Id. at 3.

MORRISON
FOERSTER