# Ransomware: A Resource Guide

**BITS Staff | November 2020**

Ransomware attacks continue to be pervasive across financial services and other critical industries and remain top-of-mind for cybersecurity leaders. BITS, the technology policy division of the Bank Policy Institute (BPI), put together the following resource guide to assist BPI members and other financial institutions prepare for cyber threats from ransomware attacks.

## Background

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems or networks, and demands you to pay a ransom for their return.[1] Ransomware is often delivered through phishing emails that appear to come from legitimate customers or contacts, which contain links or attachments that, when clicked on, may encrypt the user's computer and potentially spread to other files on the network. Incidents from ransomware can severely impact businesses processes and data necessary to operate critical services. After inflicting this damage, cybercriminals often demand a ransom payment and threaten to release stolen data if the organization refuses to pay.[2]

Ransomware attacks are on the rise and continue to target the most critical assets across industries. In 2019, the Federal Bureau of Investigation's (FBI) Internet Crime Compliant Center (IC3) received 2,047 ransomware-related complaints resulting in adjusted losses of $8.9 million, a significant increase from the 1,493 complaints received in 2018.[3] More recently, the coronavirus pandemic has provided a new opportunity for adversaries to alter attack mechanisms to target financial, health and other institutions that are working to secure the nation's most important assets. For example, the mass pivot to working from home has made banks more vulnerable to phishing attacks. According to a report by security company Arctic Wolf, the banking sector saw a 520 percent increase in phishing and ransomware attacks between March and June 2020.[4] The increased sophistication of hackers and evolution of attacks demonstrates that the situation with ransomware is not going away any time soon.

The face of ransomware continues to drive how organizational assets are protected both in preventative and response mechanisms. Financial institutions remain particularly vulnerable to ransomware attacks given the breadth of information banks store about their customers. To that end, it is crucial for organizations to develop effective response strategies to minimize the impact of ransomware attacks.

[1] See Federal Bureau of Investigation website on ransomware, available at https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

[2] Cybersecurity and Infrastructure Security Agency, Ransomware Guide, September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

[3] See Federal Bureau of Investigation, 2019 Internet Crime Report, available at https://pdf.ic3.gov/2019_IC3Report.pdf and 2018 Internet Crime Report, available at https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf.

[4] See Arctic Wolf 2020 Security Operations Annual Report, available at https://arcticwolf.com/resources/analyst-reports/security-operations-annual-report.

## Ransomware Resources

BPI-BITS compiled the following resources from U.S. government and other financial organizations to help your institutions navigate the growing threat from ransomware attacks. These resources are not intended to be all-inclusive but may serve as a foundation for managing the ransomware threat.

**Cybersecurity & Infrastructure Security Agency (CISA)**
CISA has acknowledged the recent growth in ransomware attacks across the country and throughout the world and, through their website, provides various resources and tools to help organizations guard against the ransomware threat. These resources include, but are not limited to:

- CISA Ransomware Guide – released in September 2020 by CISA and the Multi-State Information Sharing and Analysis Center, this customer centered resource guide includes best practices and ways to prevent, protect, and/or respond to a ransomware attack.
- CISA Insights – Ransomware Outbreak – issued on Aug. 21, 2019, this insights document provides recommendations any organization can take to manage their risk.
- Alerts and Statements – CISA provides a list of all alerts and statements issued related to ransomware, including information on recent ransomware attacks.
- Training and Webinars – CISA provides access to several training series and webinars on ransomware attacks and incident response.

**Federal Bureau of Investigation (FBI)**
In addition to CISA, the FBI issues ransomware-related statements on recent ransomware concerns and advisories on how to avoid and respond to ransomware attacks. The FBI's IC3 serves as a resource for filing reports on ransomware or other internet-enabled crime and uses reports to help victims of cyber crime. FBI/IC3 recent work includes:

- Ransomware Prevention and Response for CISOs – provides government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.
- High-Impact Ransomware Attacks Threaten U.S. Business Organizations (I-100219-PSA) – public service announcement dated Oct. 2, 2019 detailing information on ransomware threats, including whether to pay the ransom and how to protect your organization from ransomware.

**U.S. Department of the Treasury**
The U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence develops and implements government strategies and programs to combat terrorist financing and fight financial crimes. Treasury recently issued ransomware advisories through its Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN):

- OFAC Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments – released Oct. 1, 2020, this advisory highlights the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities.
- FinCEN Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments – released on Oct. 1, 2020, this advisory provides information on (1) the role of financial intermediaries in the processing of ransomware payments, (2) trends and typologies of ransomware and associated payments, (3) ransomware-related financial red flag indicators and (4) reporting and sharing information on ransomware attacks.

The U.S. Department of the Treasury and G7 authorities issued a statement on Oct. 13, 2020 on digital payments and the potential impact on financial stability, consumer protection, privacy, cybersecurity, operational resilience, money laundering and other issues. The statement included the following ransomware annex:

- Ransomware Annex to G7 Statement – this statement outlines the G7's concerns over malicious cyber-attacks, especially ransomware, and summarizes G7 efforts to combat ransomware.

**Securities and Exchange Commission (SEC)**
The SEC's Office of Compliance Inspections and Examinations issued a risk alert on ransomware after observing an apparent increase in sophistication of ransomware attacks on SEC registrants, including broker-dealers, investment advisors and investment companies.

- Cybersecurity: Ransomware Alert – dated July 10, 2020, this advisory provides observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency to address ransomware attacks.

**Financial Services Information Sharing and Analysis Center (FS-ISAC)**
FS-ISAC provides a platform to facilitate information sharing and consumption of cyber threat intelligence, including ransomware, across the financial industry. FS-ISAC's recent work on ransomware includes the following report:

- The Rise and Rise of Ransomware – outlines recent trends, the top five ransomware threat actors reported by members and best practices to help prevent ransomware attacks.

**Conference of State Bank Supervisors (CSBS)**
State financial regulators, joined by the Bankers Electronic Crimes Task Force and the U.S. Secret Service, issued a self-assessment tool to banks they supervise in an effort to help mitigate ransomware attacks on Oct. 13, 2020:

- Ransomware Self-Assessment Tool – this tool includes 16 questions designed to help financial institutions reduce the risk of ransomware and provides executive management and the board of directors with an overview of the institution's preparedness towards identifying, protecting, detecting, responding and recovering from a ransomware attack.
- Best Practices for Banks – CSBS and the Bankers Electronic Crimes Task Force developed this best practices guide to assist banks in reducing the risk of ransomware.

**National Institute of Standards and Technology (NIST)**
NIST's Cybersecurity Center of Excellence (NCCoE) explores methods to effectively recover from data corruption events in various Information Technology enterprise environments and issues cybersecurity practice guides on various subjects, including ransomware and other cyber threats.

- Data Integrity: Recovering from Ransomware and Other Destructive Events (SP 1800-11) – this NIST Cybersecurity Practice Guide demonstrates how organizations can implement technologies to take immediate action following a data corruption event.