

**Recommended Distribution**

Chief Executive Officer
Chief Compliance Officer
Chief Information Security Officer

Ransomware

Summary

Ransomware continues to evolve in complexity and severity across various sectors in the US. [PurpleSec](#), a leader in cyber thought leadership reports that ransomware attacks worldwide rose 350% in 2018 and costs businesses more than \$75 billion per year; 40% of ransomware victims paid the ransom. The ransom demands have also skyrocketed - the largest ransom paid being was USD 44 million.

The number of new phishing sites created each month grew to 1.5 million per month with 7 out of every 10 malware payloads delivered being ransomware. It's no wonder that 50% of 582 security professionals say they do not believe their organization is fully prepared to repel a ransomware attack.

Current trends in ransomware include the exploitation of IT outsourcing services; targeting vulnerable industries; evolving new ransomware; the spread to mobile devices, and the increasing trend of cyber-groups using ransomware as a service. (RaaS) Since these newer strains of ransomware behave differently today, there is now a need for alternate methods of detection.

On 30 August, the Securities Exchange Commission sanctioned eight firms in three actions for failures in their cybersecurity policies and procedures that resulted in unauthorized disclosure of personally identifiable information.

Account takeover, breaches, and ransomware - the FFIEC and regulatory agencies recognize that authentication considerations have extended beyond customers and include employees, third parties, and system-to-system communications resulting in increasing guideline requirements for authentication and access to financial institution services and systems to reduce risk.



Is your institution...

- *Prepared to respond to a ransomware incident?*
- *Regularly reviewing and updating your security policies and procedures?*
- *Storing, encrypting, and testing the health of your backup data?*
- *Migrating towards multi-factor authentication?*
- *Monitoring outsourced service providers and are they adhering to the same regulatory guidelines as your institution?*
- *Being kept informed about current cyber threats?*
- *Providing commercial customers with tips to prevent ransomware threats?*

For internal discussion...

- *What are the types of current threat intelligence sources your cyber-defense teams are using to detect, identify, and defend your institution against new campaigns?*
- *How did your teams perform when you tested your ransomware incident response plan?*
- *Have you established a good relationship with cybercrime law enforcement agencies before an incident occurs?*

Learn more about...

-  Strengthening your firm's defenses against ransomware ([view](#)) and tips to defend against ransomware. ([view](#))
-  The Carnegie Endowment for International Peace's cybersecurity leadership toolbox. ([view](#))

Events

CIAC Member Meeting

22 February 2022

Three-Day US Spring Summit

27–30 March 2022

Cyber-Range Exercises

Ransomware

23 March 2022

13 April 2022

26 April 2022

More info: fsisac.com/events

About FS-ISAC

Financial Services Information Sharing and Analysis Center is the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats. To learn more, visit fsisac.com.

Contact

Jeffrey Korte

Director, Community
Institution and Associations
CouncilReach out to Jeffrey on
[LinkedIn](#) 703.962.7901 ext. 583