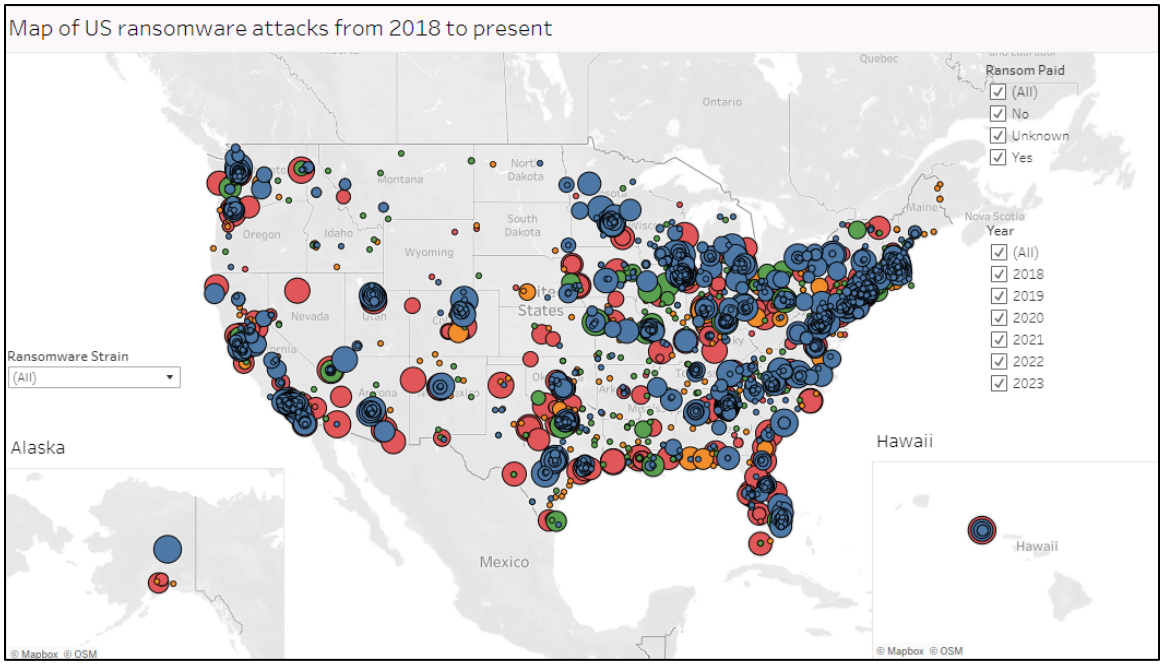
Ransomware Threats and Impacts to Industry

Cyber supply chain vulnerabilities and the rise in popularity of cryptocurrency have created the ideal environment for ransomware to flourish. Cybercriminals and malign nation-state actors recognize the value in ransomware as a revenue stream and are incentivized by their ability to obfuscate illicit transactions unencumbered by the oversight or attribution associated with traditional financial vehicles.



Comparitech hosts interactive ransomware maps, updated daily.

According to IBM Security's 2022 X-Force report, ransomware attacks made up more than 20 percent of all cyberattack types observed in 2020 and 2021. Prominent examples include: a) the attack against a German hospital in October 2020 that resulted in the first reported ransomware-connected death, b) the Colonial Pipeline ransomware attack in May 2021 that disrupted petroleum supply chains in the southeastern United States, and c) the Kaseya Limited ransomware attack launched in July 2021 against customers through a supply chain cyber attack.

To visualize the growing threat from ransomware to industry, Comparitech developed the above map to illustrate the number of ransomware attacks on key industries in the United States from 2018 to 2022. This map, and Comparitech's corresponding industry-specific reports, reveal ransomware attacks likely cost U.S. healthcare organizations more than $31 billion over the last three years. In 2020 alone, costs to U.S. businesses exceeded $20 billion. Between 2018 and October 2022, ransomware attacks on U.S.federal, state, and local government organizations exceeded $70 billion.

Ransomware actors are also increasingly targeting educational institutions. In 2021 alone, ransomware attacks cost U.S. schools and colleges more than $3.5 billion. On October 3, 2022, Russian-speaking hackers released 500GB of data stolen during a ransomware attack against the Los Angeles Unified School District (which includes more than 1,000 schools and 600,000 students) after the school district refused to pay an undisclosed ransom.

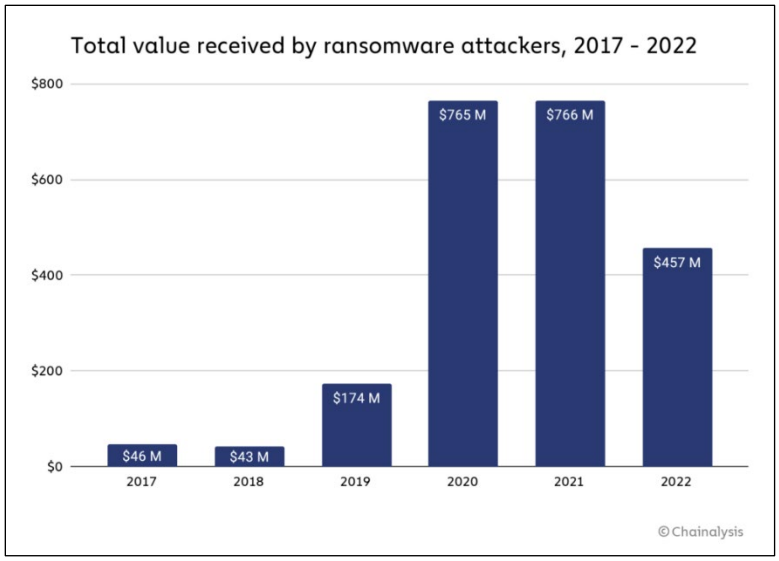
The adoption of ransomware attacks by international cyber criminals and the proliferation of Ransomware as a Service can shroud state actors in a cloak of deniability. State actors recognize ransomware can be a valuable weapon in their cyber arsenals. A ransomware attack can disrupt critical infrastructure even if—as in the case of the attack against Colonial Pipeline—industrial control systems are not breached.

Supply Chain Risk Management - A Reinforcement Against Ransomware

Since 2021, the U.S. Department of Justice (DoJ) has successfully recovered some ransomware payments by identifying and seizing accounts containing illicitly obtained funds. On June 7, 2021, DoJ announced it had seized the 63.7 bitcoin (valued then at $2.3 million) that Colonial Pipeline had paid to Russian cybercriminals. On July 19, 2022, DoJ announced the seizure of $500,000 from North Korean ransomware actors.

Despite the above successes, most ransomware payments go unrecovered, and as a result, the International Counter Ransomware Task Force (ICRTF) formed in 2023 to combat ransomware globally. The ICRTF will target ransomware through information and intelligence exchanges, by sharing best-practice policy and legal authority frameworks and through collaboration among law enforcement and cyber authorities. Chaired by Australia in its inaugural year, the ICRTF sits under the Counter Ransomware Initiative (CRI), an international body led by the United States and 37 multinational partners committed to holding ransomware actors accountable, denying them safe haven, and disrupting their financial streams.

From a cyber-supply chain risk management (C-SCRM) perspective, the CRI will promote robust and timely information sharing of "tactics, techniques, and procedures" (TTPs) and trends used by ransomware actors. Although attribution remains challenging, sharing assessed cybersecurity risks and known TTPs will reinforce the cyber supply chains of international partners and improve the CRI's ability to identify ransomware actors. In addition, the CRI will take steps to remove ransomware actors from the cryptocurrency ecosystem such as by sharing information about cryptocurrency "wallets" used for laundering extorted funds and by developing international anti-money laundering standards for cryptocurrency and related service providers. These standards will include "know your customer" rules to mitigate their misuse by cyber criminals, including those supported by nation states.



Improved system and data backup strategies gave ransomware victims better non-payment solutions in 2022.

Businesses, institutions, and individuals should not rely on the CRI's efforts alone. Rather, they should implement or reinforce their C-SCRM programs to further reduce organizational risk from ransomware attacks. The Cybersecurity and Information Security Agency (CISA) provided a Joint Cybersecurity Advisory in 2022 with suggested mitigations to guard against ransomware. Specifically, the following CISA mitigations may be incorporated into a C-SCRM program to address ransomware concerns:

- **Keep all operating systems and software up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- **Implement a user training program on ransomware.** Training programs will raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Such training reinforces the appropriate user response to phishing and spearphishing emails.
- **Employ Multi-Factor Authentication (MFA).** MFA should be required for as many services as possible particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- **Require strong passwords.** All accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) should have strong, unique passwords.
- **Enforce principle of least privilege.** Employing this principle through authorization policies minimizes unnecessary privileges for identities.