CyberSaint
SECURITY

State of Ransomware Attacks Report

CyberSaint Report 2022

Introduction

Ransomware is a form of malware that extorts victims by encrypting files on a device or server and making them inaccessible. In exchange for decryption, cybercriminals will threaten to leak or sell encrypted files in exchange for a ransom. Not only do hackers threaten to withhold files, but they can also delete systems backups. Without a backup, recovery for an organization becomes increasingly difficult or almost impossible. Ransomware is a lucrative and ever-evolving software - it can vary in its scale of attack and entry point.

When a ransomware attack occurs, businesses can lose out on more than encrypted data. A ransomware hack causes economic and reputational loss for organizations as well. Companies are left scrambling to rebuild their image and trust with their clients, and often when a company pays a ransom - there's no guarantee that companies will ever recover the files. Ransom demands have skyrocketed, with some malicious actors demanding millions. In 2021, CNA Financial reportedly paid cybercriminals $40 million in exchange for network access and stolen data. The use of this malware has grown to such an extent that there are online marketplaces for malware where hackers can buy malware kits from developers.

The extortion software can enter through a single device, but the malware can spread across networks, servers, and databases - a ransomware attack can render an entire organization powerless. The most common routes for ransomware entry are phishing scams, visiting unsecured websites, and downloading unauthorized attachments. Ransomware can also enter through unused ports and devices, dated software, loosely secured third parties, and managed service providers (MSPs).

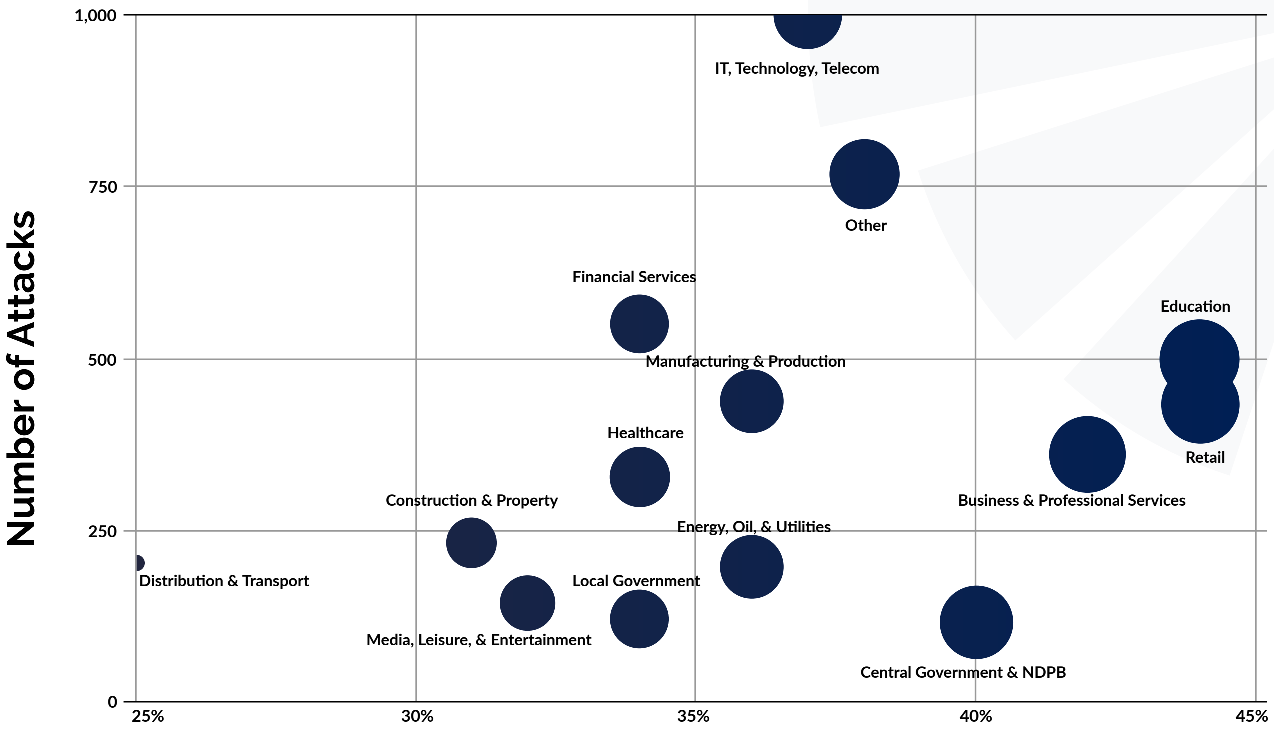
This form of malware remains undetected for as long as possible, which is why continuous vulnerability assessments are necessary. Preparing for one form of ransomware does not prepare you for other ransomware attacks. Enterprises, governments, and small businesses alike must stay vigilant and up-to-date on ransomware information and best practices. Staying informed is key to protection; organizations should engage with CISA, MS-ISAC, and Sector-based ISACs/ISAOs for ransomware updates and guidelines.

Organizations using the NIST Cybersecurity Framework can apply the NIST CSF Ransomware Profile. This gold-standard framework helps organizations identify security objectives that support ransomware prevention, responses, and recovery. The Ransomware Profile allows organizations to gauge their readiness for threat mitigation and recovery. In addition to the NIST CSF, there are several best practices to be followed like, implementing a security awareness program to ensure awareness and cyber hygiene and running secure data backups regularly. Install MFA on all services that allow, restrict user permissions to the necessary extent, and periodically remove dated software, old accounts, and unused devices.

The Current State of Ransomware

Ransomware attacks have targeted and inflicted damage at all levels of the government and across varying industries. Local government, healthcare, energy, and financial services are just a few examples of the many sectors hit with ransomware attacks. Valuable industries like critical infrastructure organizations are targeted. Since they provide vital services, organizations are more likely to pay the ransom to protect the stolen data and restore provided services. According to a poll on ransomware, 44% of respondents in the education industry reported a ransomware event. 34% of respondents in the financial services sector and local government reported a ransomware attack.

Amount of Ransomware Attacks by Industry



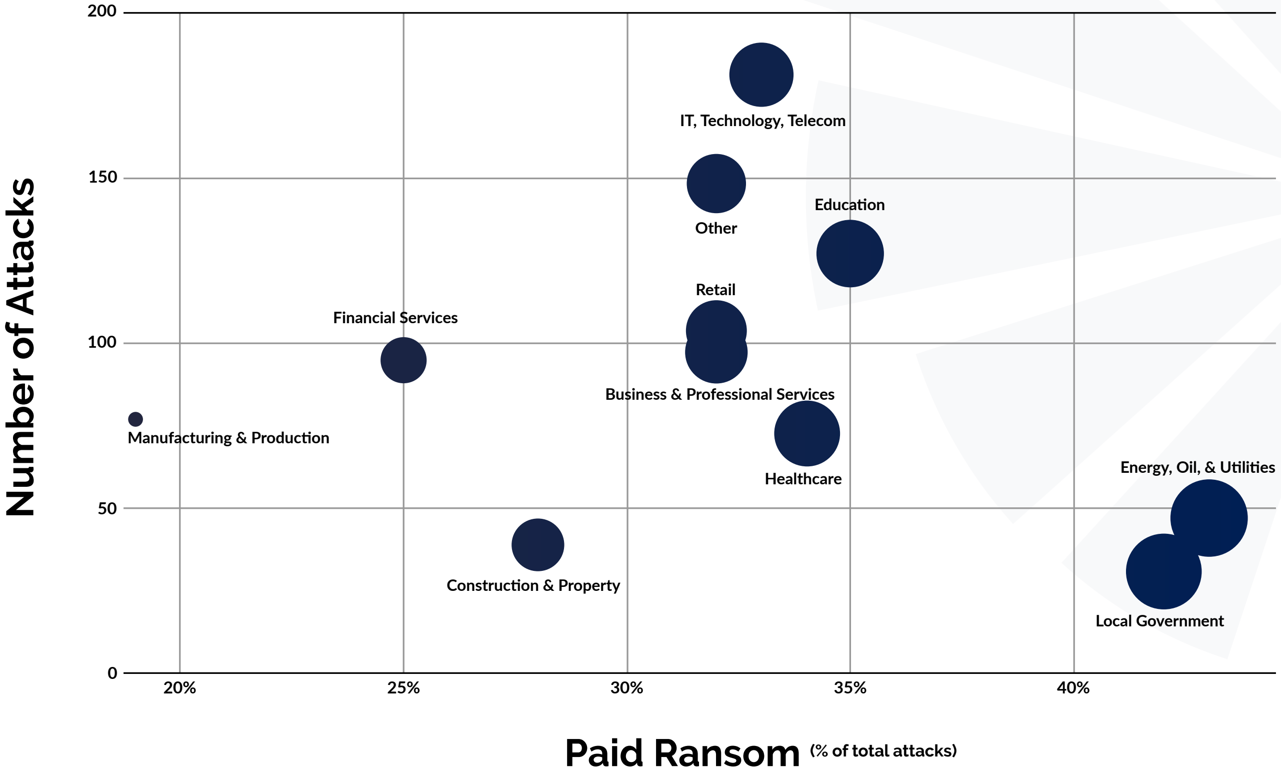
The COVID-19 pandemic has exacerbated attacks on weaker sectors like education and healthcare with remote work setups. Due to the pandemic, malicious emails are estimated to have increased by 600%. No industry is safe from ransomware threats.

As the scale and prevalence of ransomware develop, organized cybercrime groups like REvil (or Sodinokibi) and DarkSide have grown and have established unique attack tactics and targets. A group like Netwalker will typically attack through phishing emails and target industries like manufacturing, education, healthcare, and business management solutions.

The COVID-19 pandemic has exacerbated attacks on weaker sectors like education and healthcare with remote work setups.

Following some of the most significant attacks in the past year, like JBS and Colonial, public scrutiny and FBI involvement have significantly grown. Each event has left organizations and the government with several lessons to be learned as the dynamics of attacks, tactics, and pay preference were uncovered. As the world learns more and more after each episode, hackers have learned that hitting large enterprises is becoming less lucrative. It is untrue that malicious actors only target large public organizations or private enterprises. Hackers also attack small businesses and take advantage of their lack of access to ransomware remediation sources and limited public scrutiny.

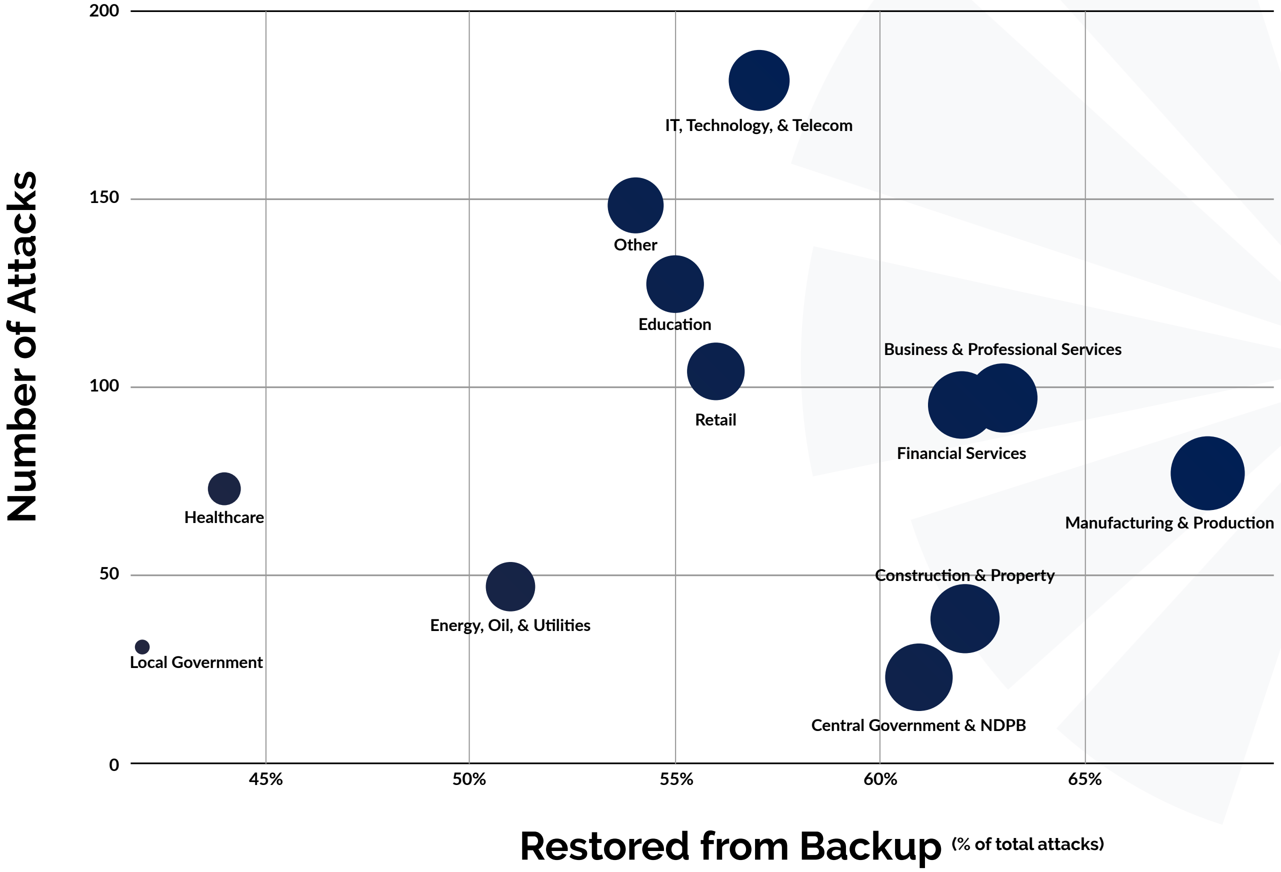
Propensity to Pay Ransom by Industry



With ransom payments increasing, small and large businesses alike face enormous demands. Across all industries, ransom payments in Q1 of 2019 averaged out to $12,762, but in just two years, in Q1 of 2021, ransom demands grew to $220,298. Without secure backups and a remediation plan, some businesses are quick to pay the ransom - not even considering that they might not recover the files. Specific industries tend to pay out the ransom more than others, like the energy, oil, and utility sector. A poll on ransomware found that, in this sector, 43% of respondents tend to pay the ransom. While energy and utilities led with their inclination to pay, other industries did not lag too far behind. Over a third of respondents in IT, retail, and business and professional services tended to pay out a ransom.

Considering a ransomware attack's economic and reputational damage, it's all hands on deck. While the CISO can be scapegoated for the security lapse, ransomware preparedness is a responsibility of all C-suite executives and the Board of Directors. When a ransomware event hits, the malware can paralyze an entire organization. Effective modern-day governance starts from the top down. Your board needs to be involved with cybersecurity decisions to get suitable investment and interest in security. A comprehensive security awareness program and remediation efforts are only possible with the cooperation of other leaders like the CEO, CIO, and board members.

Ability to Restore Data Using Backups Following Attack



Data presented as a function of total ransomware attacks in represented industries against percentage of companies able to restore data from backup. Relative size of bubbles in charts representative of percentage of companies able to restore from backup (bigger bubble, greater ability to restore from backup).

The Future of Ransomware

Across all industries, ransom payments in Q1 of 2019 averaged out to $12,762, but in just two years, in Q1 of 2021, ransom demands grew to $220,298.

Due to the success of ransomware attacks, malicious actors have developed ransomware-as-a-service (RaaS). This malware economic model allows developers to earn money by selling kits and taking a cut of the demanded ransom. Developers avoid the risk of deploying the attack while continuing to rake in profit. Whether the ransom is paid or not, this economic plan still allows developers to continue making money. RaaS establishes an infrastructure for the business of hacking and enables developers to reach a global audience rapidly. The earning potential is unlimited as demand for malware kits grows.

Using the "dark web," developers can create services like "RaaSberry," which require a subscription for access to ransomware options. Other RaaS options are more advanced and offer a control server with an administration panel for managing each victim. Ransomware attacks also target more than just data. Some ransomware attacks involve stealing organizational information and demanding another ransom to not leak the information to competitors and authorities. The pace of evolution for this malware has advanced with the availability of open-source code. So while you might learn the telltale signs of one form of ransomware, hackers are constantly developing new techniques and technology to put pressure on targets.

Instead, organizations should implement something that will mature their overall security strategy like the NIST Cybersecurity Framework Profie for Ransomware Risk Management. This profile can guide organizations in identifying security objectives and measures that support prevention, response, and recovery from ransomware attacks. The framework also aids in assessing a company's existing level of readiness for response and recovery.

The Ransomware Profile applies to organizations that have already implemented the NIST CSF and those still unfamiliar with it. The guide is also applicable to SMBs. This profile builds off of the five functions of the NIST CSF: identify, protect, detect, respond, and recover.

The Identify, Protect, and Detect Functions support prevention measures. The Identify Function helps organizations develop an enterprise-wide understanding needed to manage cybersecurity risk. Using this first foundational function, organizations will have to identify business objectives and risks, the associated cybersecurity risks, and the necessary resources to distill an effective risk management plan that prioritizes cybersecurity and business needs. This first step develops a company's focus. The Protect Function implements safeguards that ensure business continuity and supports the organization's ability to limit or contain the impact of a potential ransomware event. Protect action items include proper credential management, installing MFA, and network segmentation.

The Detect Function supports timely discovery of ransomware threats and events. Detection includes a Security Information and Event Management (SIEM) solution, continuous network monitoring, and personnel monitoring.

Developing a response plan for the business and technical side is the first step to the Respond Function. Response analysis, mitigation, and continuous improvement of the response plan are critical parts of the Respond Function. Specific action items include immediate execution of response plan to prevent data exfiltration, information sharing, and coordination with key internal and external shareholders. Mitigation plans are also a vital part of the Respond Function.

After the root cause is determined, the Ransomware Risk Profile calls for immediate initiation of a recovery plan. As defined by the NIST Profile, "The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident." Recovery involves initiating actions that maintain resilience and restore halted services. Continuous improvement of the recovery plan based on lessons learned and coordination with internal and external parties is also part of this function.

In addition to these five fundamental components, the Ransomware Risk Profile also recommends basic preventive measures like updated antivirus software, fully patched computers, restricted personally owned devices, and managing credential authorization.

Why CyberSaint

To support the continuous monitoring needed for ransomware, organizations need a platform that can support automated vulnerability assessment and network monitoring. CyberSaint's AI-assisted automation gives security teams real-time insights into risk monitoring and assessments. Manual assessments give way to human error, and with ransomware designed to remain as hidden as possible - CyberStrong and CyberBase automate assessments to mitigate control gaps and highlight critical weaknesses.

With platforms like CyberStrong and CyberBase, organizations at both the enterprise and SMB level can detect ransomware threats before they have a chance to become a full-blown event and immobilize the entire enterprise. Small businesses are often overlooked when implementing comprehensive risk management platforms. Some might think that a small business doesn't need to have the level of security larger organizations have. This is dangerous thinking. When ransomware attacks an organization, everything in its supply chain is also at risk - even with SMBs.

Like enterprises and large government agencies, SMBs also need continuous monitoring and assessment capabilities even if the scale of operations is much smaller. With CyberSaint's newest offering, CyberBase, SMBs can leverage enterprise-level risk management capabilities and reporting tools. CyberSaint's platforms arm organizations of any size with the ability to task out custom control sets to third parties and provide an infinite scale that adjusts to the size of any supply chain.