Global Ransomware Damage Costs Predicted To Hit $57B Annually In 2025

Ransomware facts, figures, predictions, and statistics for boardroom and C-Suite executives, CIOs and CISOs. Sponsored by Elastio

– *Steve Morgan, Founder of Cybersecurity Ventures*

Sausalito, Calif. – Mar. 12, 2025

Ransomware, the fastest growing type of cybercrime, is 35 years old, it shows no signs of slowing down, and it's predicted to cost victims around $275 billion annually by 2031, according to Cybersecurity Ventures, with a new attack every 2 seconds as perpetrators progressively refine their malware payloads and related extortion activities.

Ransomware costs include ransom negotiations and payouts, damage and destruction of data, stolen money, downtime, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, reputational harm, legal costs, and potentially, regulatory fines.

Adam Keown, CISO at Kingsport, Tenn.-based Eastman (NYSE: EMN), a Fortune 500 global specialty materials company, told Cybersecurity Ventures that "ransomware is a top tier concern for all CISOs at large enterprises," and that "AI has a strong potential to make ransomware more sophisticated by automating or optimizing different attack vectors."

"Ransomware isn't just an IT issue—it's a boardroom crisis waiting to happen," said Najaf Husain, founder and CEO of Elastio, a leading provider of ransomware recovery assurance. "Executives must ensure their organizations can recover, or risk catastrophic financial and reputational damage," added Husain, a well respected cybersecurity expert and entrepreneur who has watched the ransomware economy unfold over his career, which started in 1984.

2025 RANSOMWARE REPORT

Knowledge is power in the war against cybercriminals. Ransomware facts, figures, predictions and statistics with supportive information arm boardroom and C-suite executives, CIOs, CISOs, and IT and security teams globally with information for their meetings, presentations, and training programs having to do with protecting their organizations from cybercrime.

- **HISTORY.** Ransomware is 35 years old, according to CNBC, and it's come a long way since its birth date on Dec. 12, 1989, in the same year that the Internet was invented. Ransomware was originally a form of malware used by cybercriminals to lock files on a person's computer and demand payment to unlock them. Now the technology enables cybercriminals to spin up attacks much faster and deploy them across multiple targets causing far more harm. In double extortion ransomware attacks, the World Economic Forum explains, if the ransom isn't paid, the bad actors will sell the stolen data or publish it in public forums. Increasingly, cybercriminals are resorting to triple extortion, blackmailing individual employees or victims into paying for their data. Ransomware-as-a-Service (RaaS) emerged over the past few years as a cybercrime business model in which ransomware developers sell their code to other hackers, called "affiliates," who then use the code to initiate their own attacks. RaaS lowers the barrier for entry to novice and less experienced hackers with little to no programming skills, and drives many of the current ransomware attacks being launched on consumers, businesses, schools, and governments globally.

- **INVENTOR.** The first ever ransomware attack dates back to 1989, long before hackers used the internet to spread malware. The AIDS Trojan, also known as PC Cyborg, used floppy disks to target the subscriber list of a World Health Organization AIDS conference. When victims accessed the floppy disk, it released encryption malware onto their computers.The attacker then demanded $189-$378 to release the encrypted files. Law enforcement traced the effort to a PO box owned by a Harvard-taught evolutionary biologist named Joseph Popp, who was conducting AIDS research at the time. He was arrested and charged with multiple counts of blackmail, and is widely credited with being the inventor of ransomware. A technical analysis of the AIDS Information disk was published in the Jan. 1990 edition of Virus Bulletin. While the first ransomware attack had a limited economic impact, it warned computer users of the dangers of malware.

- **COSTS.** For a Board, the stakes of a ransomware attack could not be any higher. Ransomware, the fastest growing type of cybercrime, is predicted to cost its victims around $275 billion USD annually by 2031, up from $57 billion in 2025, and $20 billion in 2021, based on 30 percent year-over-year growth over a decade, due in part to the power of AI in these attacks. Ransomware gangs now routinely demand millions of dollars and will go so far as to search for revenue and insurance documents once they infiltrate a network to ascertain how much their victim is able to pay. It is critically important to remember however that payouts to perpetrators are only a small fraction of total ransomware damage costs, which are growing dramatically.

- **CALCULATIONS.** Cybersecurity Ventures publishes a chart at RansomwareCost.com containing our calculations of global ransomware damage cost predictions from 2015 to 2031. For this year, 2025, we predict that costs will reach $57 billion annually. The 2025 calculation breaks down to $4.8 billion per month, $1.1 billion per week, $156 million per day, $6.5 million per hour, $109,000 per hour, and $2,400 per second. Our first ever prediction, for 2015, put the annual cost of ransomware at $325 million. Another way to look at it is that we predict ransomware will cost the world more than $20 billion per month in 2031, up from $20 billion per year in 2021.

- **FREQUENCY.** Cybersecurity Ventures predicts that a ransomware attack will strike a consumer or business every 2 seconds by 2031, which is 43,200 attacks per day, up from every 11 seconds in 2021, which is around 7,850 attacks per day. According to INTERPOL's findings, ransomware attacks have increased by 70 percent over the past year. The actual number of ransomware attacks on individuals and organizations globally vastly exceeds the number of attacks that are reported (or even known) to media outlets, vendors, law enforcement, regulatory bodies, and industry associations. Most reporting is focused on 'corporate' attacks in developed countries that do not take unregulated and small businesses or individuals into account, let alone undeveloped countries. For every ransomware attack that is reported and counted, we believe that hundreds more go unreported. For a historical perspective, a U.S. Government interagency technical guidance document for CISOs published on the FBI website reported that on average, more than 4,000 ransomware attacks had occurred daily in 2016, up from approximately 1,000 attacks daily in 2015.

- **DOWNTIME.** Downtime from a natural disaster or ransomware can cost organizations significantly, with large businesses losing up to $357,000 per hour, according to a CIO analysis. When ransomware strikes (a disaster almost all technology leaders will experience), the disruption can last for days or even weeks. A 2024 IDC survey with 800 respondents found that approximately 33 percent of organizations experienced system or data access disruption for one week or more due to ransomware, and almost 80 percent of organizations experienced an outage of multiple days. In addition to operational downtime, the potential exposure of sensitive data, especially if it involves customers, employees, or partners, creates heightened fear and urgency.

- **RECOVERY.** Heather Engel, a cybersecurity expert and host on the Cybercrime Magazine Podcast, reported that in 2024 the average (corporate) ransom payment was around $2 million, and another $2.7 million in recovery costs, for most companies that are hit by a ransomware attack. Small businesses who are victims of ransomware are typically paying ransoms ranging from $10,000 to $100,000, according to numerous sources. Recovering from a ransomware attack was thought to be 10 times the size of the ransom payment, according to research conducted by Sophos in 2021. Cybersecurity Ventures believes that can be as high as 10 to 12 times in 2025.

- **CYBERINSURANCE.** Cybersecurity Ventures predicts the cyberinsurance market is growing from approximately $8.5 billion USD in 2021 to $14.8 billion in 2025, and will exceed $34 billion USD by 2031, based on a compound annual growth rate (CAGR) of 15 percent over an 11-year period (2020 to 2031). Some cyberinsurance policies cover ransomware negotiation and payments to hackers, but this is a controversial aspect of the coverage, as many believe it incentivizes criminals to continue launching attacks. Other policies will indemnify an organization for their cyber extortion expenses as a result of ransomware. Cyberinsurance generally does not cover stolen or damaged intellectual property, or cyberwarfare acts carried out by foreign nation state actors, both of which can result from a ransomware attack.

- **PAYOUTS.** Cryptocurrency-tracing firm Chainalysis reported that total ransomware payments were around $1.1 billion in 2023, exceeding the $1 billion mark for the first time ever, and payments declined significantly in 2024, dropping to $813 million, a roughly 35 percent decrease. And this downward payment trend occurred despite 2024 being a record year for ransomware attacks overall, according to The National Law Review. Sophos however, reported that ransom payments surged by 500 percent over the past year in its 2024 report. Either way, the numbers don't include unreported incidents and payments, which can potentially exceed those that have been reported. In the U.S., it is legal, yet controversial, to make a ransomware payment. The White House previously considered banning the practice, and paying ransoms is generally frowned upon by cybersecurity experts and law enforcement, yet there have been understandable exceptions. Payouts should never be confused with total damage costs.

- **BIG-GAME.** Bloomberg News reported in 2024 that, according to sources familiar with the situation, the Dark Angels crew received a record-breaking $75 million ransom payment for the Cencora attack and that the original demand was $150 million.The monies were paid in three Bitcoin installments. Conshohocken, Pa.-based Cencora is a global pharma giant ranked number 10 on the Fortune 500. For years prior to that, CNA Financial held the record for the biggest ransomware payout on record. In 2021, the Chicago-based insurer paid $40 million to the Phoenix cybercriminal group, believed to come from Russia. CDK Global paid $25 million to cybercriminals after a Jun. 2024 ransomware attack disrupted business for thousands of car dealerships who used its software. Change Healthcare paid $22 million in Mar. 2024 to a ransomware gang that had crippled the company along with hundreds of hospitals, medical practices, and pharmacies across the U.S. Casino operator Caesars paid out a ransom worth $15 million, half of the initial $30 million demand, to a cybercrime group that managed to infiltrate and disrupt its systems in 2023. Meatpacker JBS USA paid a ransom equivalent to $11 million following a 2021 cyberattack that disrupted its North American and Australian operations. Garmin paid a $10 million ransom to a group of Russian hackers known as Evil Corp in exchange for a decryption key to unlock files on its corporate network after a ransomware attack knocked out the GPS maker's networks for several days in 2020.

- **HALL-OF-SHAME.** Victims and gangs worldwide have achieved fame due to ransomware, the University of Tulsa explains. CryptoLocker ushered in the modern era of ransomware. From 2013 to 2014, the malware extorted $3 million from victims, and it was one of the first to demand bitcoin for its ransom. While previous ransomware attacks infected devices one by one, the 2017 WannaCry attack could spread through networks. Known as a cryptoworm, this ransomware infected more than 200,000 computers around the world. REvil (short for Ransomware Evil and also known as Sodinokibi) emerged in 2019 and netted millions using a new ransomware-as-a-service (RaaS) model. In 2021, REvil targeted a remote network management company, infecting over a thousand business networks around the world. In 2021, a ransomware attack targeted Colonial Pipeline, the largest refined products pipeline in the U.S., leading to a shut down of the pipeline for nearly a week, causing gas shortages and leading to a state of emergency in 17 states. In Oct. 2023, a cyberattack took down the British Library (the national library of the UK) website for months. Attackers stole personal data and threatened to sell it online, known as double extortion. In Oct. 2023 Progress Software disclosed that it had received a subpoena from the SEC to share information relating to the vulnerability in its file transfer software, MOVEit, which became the subject of a massive exploit beginning months earlier. One report estimated that the MOVEit breach exposed the information of at least 64 million individuals through 2,547 affiliated organizations. The culprits of the attack, the CL0P ransomware gang, "helped pioneer the practice of double-extortion," according to Reuters. A partial list of others in the hall include Maze, Cuba, DoppelPaymer, Ryuk, Netwalker/UCSF, GandCrab, SamSam, Locky, Royal, Rhysida, ESXiArgs, ScatteredSpider, NotPetya, WizardSpider (aka Trickbot), DarkSide, Hunters International, and Hive.

- **GANGS.** A 2025 feature in CSO, “The dirty dozen: 12 worst ransomware groups active today”, highlights the cybercriminal gangs currently responsible for causing the most damage insofar as ransomware goes. The gangs named are (in alphabetical order) Akira, Black Basta, Blackcat (aka ALPHV), BlackLock, Cl0p, Funksec, Lockbit, Lynx, Medusa, Play, Qilin, and last but certainly not least, RansomHub, who The Hacker News called 2024’s top ransomware group, hitting more than 600 organizations globally. There are no specific numbers of ransomware gangs, but as far back as 2021 the FBI was tracking more than 100 active gangs. Some media outlets put the current figure at anywhere from 50 to 100 ransomware groups. For any perceived decrease in the number of gangs, it’s important to point out that a group may shut down only for its members to join another group, or to start up their own group.

- **AI.** A new ransomware group, FunkSec, has emerged as a growing concern for its use of artificial intelligence (AI) to enhance its tools. The group debuted in late 2024 and quickly claimed more than 85 victims globally. Researchers at Check Point have highlighted FunkSec’s unique approach, which combines novice tactics with advanced AI capabilities to blur the lines between hacktivism and cybercrime. The rise of Funksec’s ransomware, which focuses on extortion through file encryption and data theft, shows how LLMs are empowering ransomware groups. Funksec’s meteoric rise to the top of ransomware statistics, despite an apparent lack of experience, proves that LLMs are lowering the skill barrier for threat actors to succeed in the ransomware game.

- **LAWSUITS.** If a company doesn’t pay a ransom and suffers damage as a result, then they may also be at risk of legal fees that far exceed the ransom demand. A notable example is Lehigh Valley Health Network. CNBC reported that in 2023 the Pennsylvania-based hospital refused to pay a $5 million ransom to the ALPHV/BlackCat gang, leading to a data leak affecting 134,000 patients on the dark web, including nude photos of about 600 breast cancer patients. The fallout was severe, resulting in a class-action lawsuit. LVHN agreed to settle the case for $65 million. Scottsdale, Ariz.-based SimonMed Imaging, which employs around 200 radiologists working across 170 sites in 11 states, allegedly failed to protect patients' personal information ahead of a recent ransomware attack, according to Radiology Business. The practice claimed it had interrupted hackers before they encrypted data. A Maricopa County resident filed suit against SimonMed seeking a jury trial and damages of more than $5 million. The hacker group Medusa claimed credit for the attack, contending it has hundreds of gigabytes of data from the practice's patients. Plaintiff attorneys claim at least 132,000 individuals were impacted by the incident. They're seeking punitive damages, attorney fees, a declaratory judgment and injunctive relief. In Jan. 2025, MGM Resorts International agreed to pay $45 million to settle multiple class action lawsuits related to a data breach in 2019 and a ransomware attack the company experienced in 2023. These matters barely scratch the surface of lawsuits resulting from ransomware attacks.

- **LAW-ENFORCEMENT.** For the last full year tracked, the FBI's Internet Crime Complaint Center (IC3) handled 2,825 ransomware complaints. The FBI conducted more than 30 disruption operations last year in which officials targeted the infrastructure used by those groups. In 2024, law enforcement from 10 countries disrupted the criminal operation of the LockBit ransomware group, widely recognized as the world's most prolific and harmful ransomware, causing billions of euros worth of damage. The international sweep followed a complex investigation led by the U.K.'s National Crime Agency in the framework of an international task force known as 'Operation Cronos', coordinated by Europol and Eurojust. The months-long operation included the takedown of 34 servers in the Netherlands, Germany, Finland, France, Switzerland, Australia, the U.S. and the U.K. A cybercrime-focused division of the U.S. Department of Homeland Security said in Oct. 2024 it had disrupted more than 500 ransomware attacks and seized billions of dollars in cryptocurrency since 2021. In Mar. 2025, the U.S. Secret Service seized the domain of the Russian cryptocurrency exchange Garantex, which was previously sanctioned by the Treasury Department's Office of Foreign Assets Control (OFAC) in Apr. 2022 after over $100 million in Garantex transactions were linked to darknet markets and cybercrime actors, including the notorious Conti Ransomware-as-a-service (RaaS) operation.

- **CYBERWARFARE.** In May 2024, Reuters reported U.S. officials confronted the Chinese government in Beijing about a sweeping cyber espionage campaign through which Chinese hackers broke into dozens of American critical infrastructure organizations. Under the campaign named Volt Typhoon, American officials said China aimed to leverage the access it had gained into U.S. organizations in the event of a war or conflict. Though Volt Typhoon doesn't directly deploy ransomware, it operates within an ecosystem transformed by Ransomware-as-a-Service (RaaS). In 2022, a ransomware attack targeted the government of Costa Rica. In response, the country declared a state of emergency. The attackers demanded a $20 million ransom and threatened, "We are determined to overthrow the government by means of a cyberattack, we have already shown you all the strength and power." The extortion attack signaled to governments around the world that ransomware could pose a major national security threat. The FBI reported that government entities, including U.S. states and cities, and foreign nations, were the third most-targeted sector by ransomware in 2023. The computer systems of Swedish government agencies were made inoperable by an attack on a Tietoevry Oyj data center that was down for weeks in 2024. A ransomware attack by the Akira group crippled payroll processing at a large number of institutions, and caused additional problems at hospitals, cinemas and other businesses in Sweden. Over the past year, Cybercrime Magazine has tracked ransomware attacks on the U.K., Singapore, Hungary, Slovakia, Indonesia, Vietnam, Switzerland, Australia, Romania, and others.

- **AUTOMOTIVE.** CDK Global, a company that provides auto dealerships across the U.S. with software for managing sales and other services suffered a ransomware attack, prompting the company to temporarily shut down most of its systems on Jun. 19, 2024, effectively preventing about 15,000 car dealerships from making sales. The following month, Michigan-based Anderson Economic Group (AEG) estimated the first two weeks cost dealers more than $600 million, and could have potentially reached up to $1 billion. In Jul. 2024, three sources closely tracking the incident confirmed to CNN that a roughly $25 million payment had been made and CDK said that it was bringing car dealers back online to its software platform. One of the largest car dealerships in the U.S., Sonic Automotive, said the IT outage caused by CDK Global's ransomware attack cost it approximately $30 million. The CDK hack was a wake-up call for every auto manfucturer and dealership who was not already paying attention to ransomware.

- **HEALTHCARE.** Hospitals and health systems globally have been in critical condition and recovery due to ransomware infections. Ransomware has even led to an increase in mortality rates among hospitalized patients in 2024. Healthcare IT News reports that in the healthcare industry alone, ransomware has caused nearly $22 billion in downtime losses over the last six years. There's been a 300 percent increase in ransomware attacks on healthcare since 2015, according to IBM. In the last fiscal year, nearly 400 U.S.-based healthcare institutions were successfully hit with ransomware, causing "network closures, systems offline, critical medical operations delayed, and appointments rescheduled," Microsoft said in its annual Digital Defense Report. The largest ever ransomware attack last year against UnitedHealth Group subsidiary Change Healthcare exposed data of more than 190 million people — up from previous reports of 100 million — according to the American Hospital Association.

- **MANUFACTURING.** Manufacturing is the most targeted sector for cyberattacks for three years in a row, according to a World Economic Forum article by Blake Moret, CEO at Rockwell Automation and Kiva Allgood, Head, Centre for Advanced Manufacturing & Supply Chains, Member, Executive Committee, at WEF. It now accounts for nearly 26 percent of attacks, with ransomware involved in 71 percent of these incidents. Manufacturing makes up the biggest percentage of Microsoft's ransomware incident response engagements at 34 percent. Industrial cybersecurity firm Dragos reported an

87 percent increase in ransomware attacks against industrial organizations over the past year and a 60 percent rise in ransomware groups affecting OT/ICS (operational technology/industrial control systems) in 2024. Trustwave SpiderLabs' manufacturing research, released in Feb. 2025, finds that 54 percent of ransomware attacks were in the U.S.; 19 percent of ransomware attacks were conducted by Play; 14 percent of ransomware attacks targeted machinery manufacturers; 87 percent of attacks originated from phishing; and 86 percent of credential access techniques were brute-force attempts. Arctic Wolf reports on staggering losses suffered by alleged ransomware victims in the manufacturing industry including: Clorox in 2023 for $356 million; Applied Materials in 2023 for $250 million; Johnson Controls in 2023 for $27 million; JBS in 2021 for $11 million; Norsk Hydro in 2019 for $70 million; and Mondelez International in 2017 for $100 million.

- **FINANCIAL-SERVICES.** In Aug. 2024, a bipartisan pair of lawmakers on the U.S. House Financial Services Committee sounded the alarm about ransomware attacks on financial institutions, pushing in new legislation for more coordination between the public and private sectors on prevention and response measures. Trustwave's recent Risk Radar Report put out the following research: 65 percent of ransomware attacks targeting financial services were in the U.S.; 20 percent of ransomware attacks in the sector were against banking institutions; and 24 percent of ransomware attacks against the financial sector were by ALPHV. A Sophos report found that 65 percent of financial services organizations were hit by ransomware in 2024. A few examples illustrate the global crisis. Reuters reported that nearly 300 small Indian banks were forced to go offline due to a ransomware attack in Aug. 2024. Dublin, Calif.-based Patelco Credit Union, which has around 9 billion in assets and 37 branches throughout the Bay Area, was hit by a ransomware attack in Jul. 2024, shutting down some of its systems for two days. As a result, one of its San Francisco locations limited customer withdrawals to $500. Bank members were left wondering when they'd be able to access all of their funds. Around 60 credit unions were dealing with outages due to a 2023 ransomware attack on a widely-used technology provider not long after the National Credit Union Administration (NCUA) warned that it was seeing an increase in cyberattacks against credit unions, credit union service organizations (CUSO), and other third-party vendors supplying financial services products. A 2025 ENISA (European Union Agency for Network and Information Security) overview of rising cyber threats in Europe's financial sector highlights that ransomware groups have evolved their tactics, employing double extortion schemes, where stolen data is leaked if ransom demands are not met.

- **MUNICIPALITIES.** Municipalities are notoriously understaffed, underfunded, and possess little training when it comes to cybersecurity preparation and mitigation. More than 400 ransomware attacks hit city and county governments in the U.S. between 2016 and 2021, according to the Washington Post. Wilmer, a town of almost 5,000 people just south of Dallas, is one of 22 cities across Texas that The New York Times reported were simultaneously being held hostage for millions of dollars after a sophisticated hacker, perhaps a group of them, infiltrated their computer systems and encrypted their data. The 2019 attack instigated a statewide disaster-style response that included the National Guard and FBI. In 2022 alone, 106 U.S. Governments were hit, including a ransomware attack that plunged Long Island's Suffolk County into the 1990s. A frantic push to counter the threat hobbled the county, as officials disabled email for all 10,000 civil service workers. Emergency dispatchers had to take down 911 calls by hand, Police officers were radioing in crime scene details, rather than emailing reports to headquarters, and office workers resorted to fax machines. The Record reported that there were 256 publicly announced ransomware attacks against state and local governments in 2023, but this is hardly just a U.S. problem. In 2023, a ransomware attack paralyzed local government services in multiple cities and districts in western Germany. An unknown hacker group encrypted the servers of the local municipal service provider Südwestfalen IT. To prevent the malware from spreading, the company restricted access to its infrastructure for over 70 municipalities. The attack left local government services severely limited, and nearly all town halls in the region were impacted by the hack. Government agencies topped the list of ransomware attacks in 2024, according to Sophos. A 2025 University of Maryland research paper in the Journal of Cybersecurity measures cyberattack vulnerability for every U.S. state and region, something that was previously considered to be a black-box, and that may shed light on which U.S. cities are at the greatest risk of ransomware.

- **CRITICAL-INFRASTRUCTURE.** Critical infrastructure, according to Palo Alto Networks, includes all of the assets, systems and networks – physical and virtual – that are essential to the proper functioning of a society's economy, national public health or safety, security, or any combination of these. In Sep. 2019, Philadelphia, Pa.-based Temple University started a dataset of Critical Infrastructures Ransomware Attacks (CIRAs). These are based on publicly disclosed incidents in the media or security reports. The dataset has nearly 2,100 records (as of Mar. 2025) assembled from publicly disclosed incidents between Nov. 2013 and Jan. 31, 2025. The data shows that the three most targeted critical infrastructure sectors/subsectors from two years ago remain popular today: government facilities, healthcare and public health, and education facilities. The CIRA data shows an increase in larger ransom demands compared to two years ago. The cost of recovering from ransomware attacks has quadrupled for organizations in critical infrastructure industries, with the median recovery cost for such organizations hitting $3 million in 2024, according to Sophos. Federal News Network reports that according to one estimate, out of the ransomware attacks that occurred over the last year, a staggering 88 percent were launched against organizations in critical sectors. The five top ransomware variants infecting critical orgs, as reported to the FBI's IC3, were LockBit, ALPHV/Blackcat, Akira, Royal, and Black Basta. The FBI and CISA recently warned that the Ghost ransomware has hit firms in over 70 countries. A joint security advisory noted that the groups are mostly targeting critical infrastructure organizations. Dubai-headquartered multinational energy services supplier Halliburton revealed late last year that an Aug. 2024 ransomware breach cost the firm $35 million, highlighting the major financial impact of attacks on critical infrastructure.

- **EDUCATION.** Moody's Ratings, a global credit rating provider, said in 2024 that the education sector has reported one of the highest rates of ransomware attacks. In its 2024 threat assessment report, the U.S. Department of Homeland Security declared K-12 school districts "a near constant ransomware target." The report attributed this alarming trend to budget constraints within school IT departments, insufficient dedicated cybersecurity resources, and the troubling success cybercriminals have had in persuading schools to pay ransoms. Ransomware has ballooned in the K-12 sector over the last seven years, according to the K12 Security Information eXchange. The recent hack of U.S. edtech giant PowerSchool is on track to be one of the biggest education data breaches in recent years. PowerSchool, which provides K-12 software to more than 18,000 schools across North America, first disclosed the data breach in Jan. 2025. The PowerSchool hack seems to have been much worse than originally believed, as new reports now claim more than 62 million students, and nine million teachers, were actually affected. Although it was not widely reported as a ransomware attack because data was not encrypted, PowerSchool reportedly paid a ransom to prevent attackers from releasing stolen data of students and teachers. In 2022, 157-year-old Illinois-based Lincoln College, a small school of less than 1,000 students, became the first American college to announce permanent closure due in part to a ransomware attack on the school. While not all attacks on universities are as dire as that, they are nonetheless threatening higher education globally. In 2024 Sophos reported in its latest survey that 66 percent of higher education organizations were hit by ransomware attacks, and 98 percent engaged with law enforcement and/or official government bodies following an attack.

- **SUPPLY-CHAIN.** As organizations become more interconnected and rely on centralized systems, they're increasingly vulnerable to ransomware attacks. One of the most notable ransomware attacks of 2024 targeted Blue Yonder, a supply chain software company, resulting in widespread fallout with two of its biggest clients: Starbucks and Morrisons, a large U.K.-based supermarket chain. Supply-chain ransomware attacks are especially damaging as they have ripple effects not only across the targeted organization, but throughout the industry they serve, according to Norton. In 2023, over 60 credit unions across the U.S. were taken offline following a ransomware attack at one of their technology providers. In 2021, Kaseya sustained a ransomware supply chain attack in which the attackers leveraged Kaseya VSA software to release a fake update that propagated malware through Kaseya's managed service provider (MSP) clients to their downstream companies. Russia-based REvil group claimed responsibility and demanded $70 million in exchange for decrypting all affected systems. Kaseya announced it acquired a universal decryption key and was offering it to customers. Many firms had already restored their systems from backups, and some reportedly already negotiated individual ransoms, paying between $40,000 and $220,000, according to the U.K.'s National Cyber Security Centre (NCSC).

- **SMALL-BUSINESS.** According to Ricoh USA, small businesses have seen a 40 percent increase in ransomware attacks, and SMBs (small-to-midsized

> businesses) with revenue around $5 million are twice as likely to become victims as companies in the $30-50 million range and five times as likely as companies with revenue of $100 million. A recent Forbes article calls small-to-medium enterprises (SMEs) the new primary ransomware target and points out that the consequences can be catastrophic, with 60 percent of small businesses shutting their doors within six months of a major cyberattack, according to Cybersecurity Ventures. KnowBe4 reports that in 2024, half of all ransomware attacks targeted small businesses, who aren't prepared, as one in five paid the ransom to recover their data, 22 percent higher than the average. There are some ransomware groups, for example CosmicBeetle, a RansomHub affiliate, who specialize in targeting small businesses.

For the latest ransomware attacks and daily news covered by Cybersecurity Ventures, visit RansomwareNews.com.

– *Steve Morgan is founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine. The 2025 Ransomware Report is published by Cybersecurity Ventures.*

SPONSORED BY ELASTIO

Founded in 2020, Elastio was created to address the growing threat of ransomware and ensure businesses can protect and secure their most critical asset: their data.

Our team brings decades of expertise from leading organizations in data protection, security, and threat intelligence, including Fortune 500 companies.

Guided by Zero Trust principles, Elastio assumes that workloads and data can be compromised at any time. Unlike other solutions, Elastio inspects data off the host, preventing tampering and ensuring businesses always have secure, clean, and ransomware-free data. This approach delivers unparalleled confidence, enabling organizations to recover quickly and without compromise, even in the face of advanced attacks.