# CIOs Have It Wrong When It Comes to Ransomware

## Why We Need To Rip Up the Current Playbook and Rethink This Threat, and Our Response to It

Ryan Cote, Global CIO
2023

I've been in the IT business for nearly 30 years; I've seen and done a lot in that time as it relates to cyber threats and it's hard to admit when I'm wrong. But it's time we shift perspective as an industry and take a fresh approach to how we're dealing with ransomware.

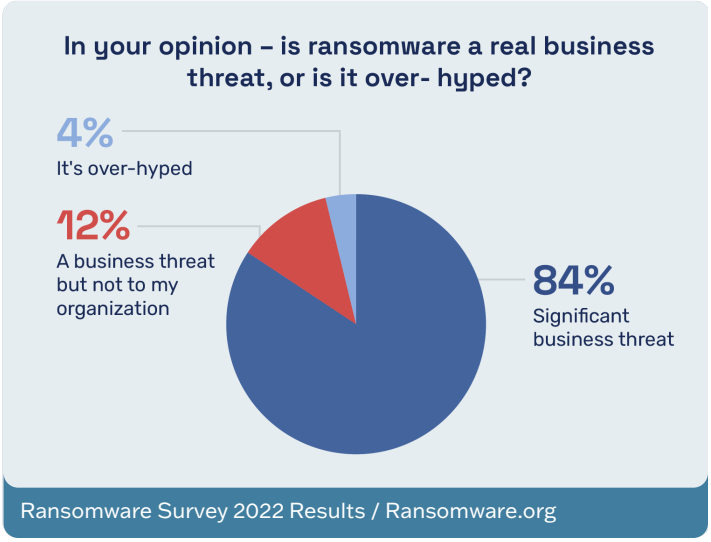
Many current cyber experts might be surprised to learn that ransomware has been around since 1989 (us old-timers remember the 80s). The first known occurrence of ransomware, AIDS Trojan, was written and deployed by a disgruntled Harvard grad and evolutionary biologist Dr. Joseph Popp. Popp, sent out roughly 20,000 floppy disks to attendees of the World Health Organization's AIDS conference infected with a piece of encryption malware. Once active, the disk-based malware program would log the number of times the computer was booted. When the boot-count reached 90, file directories would be concealed with the files either becoming locked or encrypted. To recover access to the files, $189 needed to be sent to a PO box in Panama addressed to the PC Cyborg Corporation.

Nobody knows exactly how many computers were infected by AIDS Trojan or what the monies paid to Popp totaled. The risk of AIDS Trojan in the end was minimal because it used symmetric cryptography. Tools quickly emerged that could decrypt the files without payment. Jim Bates, editorial advisor for Virus Bulletin, authored the programs AIDSOUT and CLEARAID in January 1990. The programs, respectively, removed the malware from the computer and decrypted the files, making them usable again. [1] It's worth noting that while this menace has been around for a long time, and has gotten exponentially more sophisticated, the basic threat architecture and attack vector has remained the same; unwanted, unsanctioned, unauthorized, and highly undesirable file encryption. Data exfiltration held for ransom is a separate topic for another day.

The risk of becoming a victim of ransomware today could not be greater. Up to 1,981 schools, 290 hospitals, 105 local governments, and 44 universities and colleges were hit with ransomware in the U.S. alone during 2022, demonstrating how ransomware attacks remain a significant cyber threat to the public sector and civil society. [2] It appears that only a marginal number of ransomware attacks on private sector companies are publicly disclosed or reported to law enforcement, which results in a lack of reliable statistical information in that arena. Most cyber experts agree that ransomware attacks continue to increase, ransom demands continue to rise, and levels of complexity and cleverness change and become more challenging to detect and prevent.

The 2022 ransomware.org survey of IT and security industry professionals offers valuable insights into the current state of ransomware. [3] My biggest takeaways are that 84% of those surveyed believed the threat will remain high or increase in 2023 and that it represents a "significant business threat" to their enterprises. They're not wrong. In fact, Paul Furtado, Gartner Research Vice President, recently summarized the gravity of this issue:

> *"Ransomware attacks are really not a one-off situation, we're at a point now where we just have to accept that they are going to happen."*



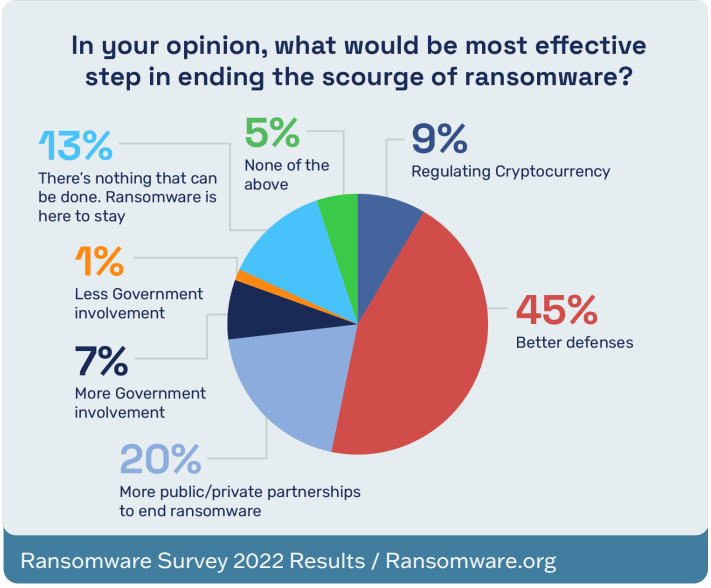
64% of respondents believed that if attacked, recovery will take days or weeks. Once again, they're not wrong (In fact, the average recovery time is 20 days). [4] Nearly 50% of respondents, an alarming number, believe that the most effective means of combating ransomware is "better defenses." While defenses, defense modernization efforts, and cyber projects remain critical to success, it's worryingly naïve to think this will provide the "most effective" steps to ending ransomware. IT spending on building better cyber defenses has reached its highest rate ever. The overall spending % of IT budgets dedicated to cyber tools and defenses has exploded over the past decade. Global cybersecurity spending will exceed $1.75 trillion from 2021-2025. [5] We must admit that this is not effective enough. If it was, we'd see the number of successful attacks decreasing year over year. The opposite is happening.

Bad actors and ransomware gangs are exploding in number because success drives success. Criminal marketplaces such as Genesis enable entry-level cybercriminals to purchase malware and malware deployment services and sell stolen credentials and other data in bulk. Access brokers are increasingly selling vulnerable software exploits and credentials to other criminal organizations. These "precursor" tools allow threat actors to easily deploy malware to both spread laterally and escalate access before a ransomware package is deployed. This means disabling backups and snapshots (a primary strategy in ransomware recovery) and maximizing impact and damage to the enterprise.

This industrialization of ransomware has allowed ransomware "affiliates" to evolve into professional operations specializing in exploitation. These professional groups specialize in gaining (or purchasing) access for any motivated actor willing to pay—or, in some cases, multiple actors with multiple motives.

> The risk of becoming a victim of ransomware today could not be greater. Up to 1,981 schools, 290 hospitals, 105 local governments, and 44 universities and colleges were hit with ransomware in the U.S. alone during 2022.

The ransomware gangs or threat actors are attacking more every day. Those attacks are increasingly successful, and they're getting paid hundreds of millions of dollars in ransoms. If they weren't, they'd stop and find something else more lucrative to do with their time. According to cybersecurity firm CrowdStrike, "Over the last several years, adversaries that engage in ransomware have advanced rapidly in terms of their capabilities and sophistication. It is reasonable to expect that this trend will continue at an accelerated rate with the same goal in mind – to apply as much pressure as possible to organizations to pay ever-larger extortion demands." [6]



Ransomware Survey 2022 Results / Ransomware.org

This growth is tied to their success, which is attributable to our failure as an industry to fundamentally grasp the problem and deploy the most effective solution. If ransomware, as defined earlier as an unsanctioned encryption is the problem, then the only sensible solution to combat this crippling threat is sanctioned decryption.

Nearly 80% of participants from the ransomware.org survey said that their data storage and backup strategy is "moderately to highly" ransomware-proof and that it represents their primary or only method or plan for recovery once becoming a victim of ransomware. I believe this widespread mindset and ransomware mitigation strategy is unfortunately accurate and fatally flawed.

First of all, no data backup or storage solution is "ransomware proof." That's a pipe dream. Anyone selling that promise should be permanently removed from an active 3rd party vendor list because they're lying. All modern backup and data storage solutions on the market rely on agents to facilitate communication between hosts and data targets. Even the so-called "agentless" solutions (For virtual environments primarily) require a centrally located "intelligence" server to manage disk-to-disk image snapshots and backups. In other words, all of these solutions require network level communication between endpoints, servers, hosts, targets, disks, tape, etc. to facilitate their image creation and exports. These communications can be and often are easily disrupted and/or disabled by threat actors early upon entry into the environment. The same threat actors that have penetrated defenses many believed

were sufficient. Do you really believe that once they're inside the walls they're not going to move laterally and disrupt your plans for recovery? If they were smart enough to circumvent and breach cyber defenses undetected, do you not think they're smart enough to disable or significantly corrupt your backup infrastructure or environment?

These so-called backup solutions are the first thing ransomware gangs silently attack well before they ever detonate the ransomware payload. Once ransomed, most organizations are shocked to find that their backup/DR response plans are entirely ineffective because the reliance on backups was grossly miscalculated. In fact, that is why statistics show 72% of organizations attacked by ransomware pay the ransom. This statistic is staggering. Whether attributable to misplaced confidence, arrogance, complacency or lack of knowledge; centering a ransomware recovery strategy and response around recovering from backups is simply foolish and impractical in today's modern IT landscape. To prove this point, let's walk through a typical ransomware prevention strategy, then an attack and typical response. As a CIO or CISO, typical ransomware prevention strategy looks like this:

- Stop attacks preemptively with defenses. (Proven by current victim statistics to be false.)
- If they get through, restore from backups. (Proven by 72% ransom payment rate to be false.)
- If the backups fail, pay the ransom. Takes on average 10-15 days to negotiate and make the payment. I'm negotiating (trusting) criminals to return my data (and encryption keys), and have to accept 35% average data corruption rate.
- Rebuild from older, non-corrupted or encrypted backups and accept the data loss. (This can take months if it's possible at all.)
- Accept the nearly 100% data/system losses and start over. Can the business survive such a protracted outage?

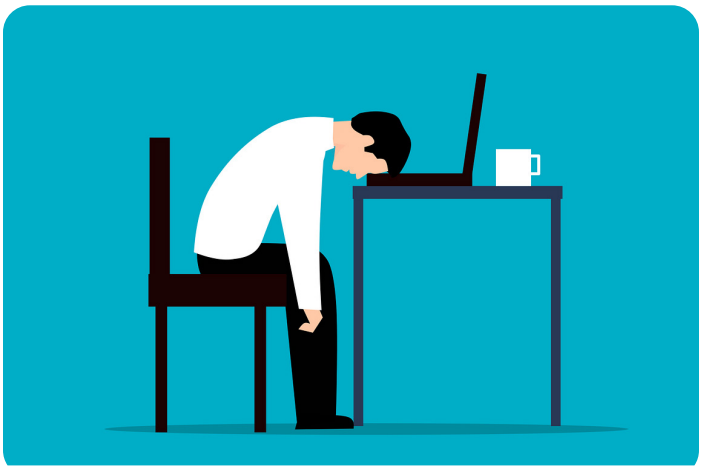
As if all this bad news isn't enough, arguably the single most important reason we need to re-think our approach to ransomware is the serious shortage of cyber talent in our industry and the fact that the ones we have are getting stressed and burned out. According to the 2022 Cyberthreat Defense Report published by the CYBEREDGE Group [7], four out of the Top Five insights or takeaways for 2022 are directed related to this problem:

1. **There has been no let-up in pressure on security teams.** While the number of organizations that experienced a successful cyberattack dropped a touch from 86.2% in the previous survey to 85.3% in this one, the percentage victimized by six or more attacks increased to a new record of 40.7%.

2. **The biggest security issues for many organizations are a persistent shortfall of skilled IT security personnel and low security awareness among employees.** These continue to top the list of factors that inhibit organizations from adequately defending themselves against cyberthreats.

3. **Among cyberthreats, ransomware and account takeover (ATO) attacks are poised to overtake malware as the #1 concern.** Malware is still perceived as the most important threat, but ATO and credential abuse attacks moved up from fourth place last year to #2 this year, and ransomware is only a tad behind.

4. **Pressure from ransomware rachets up once again.** The percentage of organizations victimized by a ransomware attack in the past 12 months rose 2.5% to reach a new high of 73%. Ransom demands continued to rise, and the percentage of organizations deciding to pay jumped from 57% to 72%, also a record. The data also points to a "sweet spot" for ransomware gangs: organizations with 5,000 to 25,000 employees.



These overworked, stressed and burned-out security engineers are the ones that need to be at their best to engineer and manage our SOCs and cyber defenses, mitigate our risk, and, frankly, save our jobs. Instead, they are asked to do more and more and face an ever-increasing threat with old strategies and thinking. A 2022 report from CPO Magazine reports that 80% of security engineers report feeling "some level of burn out," and that 67% plan to leave their current job in the next 12 months, citing low pay and "low satisfaction around the tools they use or have access to." [8]


There is hope however. And this is where the ransomware playbook has to change. Multilayered defenses are still a must. You have to protect your environment, infrastructure and particularly the data at every turn. Endpoint protection, DLP, CASB, firewalls, snapshots, backups, etc. It all remains critical to having a mature and robust cybersecurity strategy, but I now see that an additional and new layer is available to us and essential to combat ransomware specifically.

> These overworked, stressed and burned-out security engineers are the ones that need to be at their best to engineer and manage our SOCs and cyber defenses, mitigate our risk, and, frankly, save our jobs. Instead, they are asked to do more and more and face an ever-increasing threat with old strategies and thinking.

Around 18 months ago, a colleague of mine asked me to look at a new and emerging technology related to ransomware. When I met the founders and examined their tech, my first reaction was "%$@^#*! This is not possible!" But as I dug deeper into their solution, spent more time learning and understanding what they were doing, I eventually was convinced that they had found the first modern solution to ransomware.

Nubeva is a team of encryption experts who have figured out the most obvious solution to an issue that has been plaguing our industry now for more than 30 years. If bad guys want to illegally and undesirably encrypt my files for ransom, why not simply decrypt the files myself? Until now, that wasn't possible because we need the encryption keys. And we'd have to pay for those, right? Nubeva has figured out a way to silently and securely copy ransomware encryption keys during a ransomware attack and retain a copy to use to unlock my files.

It's such a simple and elegant solution that my initial reaction was, "It can't be that easy." (And technically speaking it's not actually easy. But the brains at Nubeva are really, really smart). Nubeva can somehow distinguish between known good encryption (think Bitlocker, Trend Micro, etc.) from bad encryption (LockBit, Conti, Hive, etc.) and when they detect said "bad" encryption, they quickly capture the keys and save copies (multiple copies for good measure) to return to you and instantly decrypt your files.

CIOs, trust me, I know it sounds too good to be true. But take my word for it. Better yet, go check it out for yourself. **https://www.nubeva.com/ransomware_reversal**

Do yourself and your organization a favor and re-think how you're approaching the ransomware threat. Tear up the old playbook, challenge yourself to re-think what you once knew. Your security engineers will thank you; Your CEO will thank you; Your entire organization will thank you and soon realize you're the only reason they're still in business after you survive the upcoming ransomware attack you know is coming. Your data resiliency strategy cannot be dependent simply on backups or snapshots. Protect your data from ransomware attacks the only way it makes sense. Decryption. ■

## EPILOGUE:

Full transparency, I now act as an official advisor to Nubeva. This role is not in conflict to anything I've written above. My intention in authoring this editorial is simply to make my fellow CIO colleagues aware of a new and emerging technology that I strongly believe they need to consider adding to their overall data resiliency strategy.

Additionally, I have to give another shout out to my former Gartner colleague, Paul Furtado. His short video https://www.youtube.com/watch?v=ohjgHppIOcU on understanding and preparing for a ransomware attack is worth watching. Business and IT leaders alike would be wise to heed his advice.

**Some of my favorite quotes of his from the video include:**

"Unlike any other sort of security incident that occurs, it puts your business on a countdown timer. Any delays in the decision-making process are going to introduce additional risk to the business and potentially additional cost".

"In the middle of a ransomware event, it quickly shifts from how much is this going to cost to how long is it going to take to fix? The bad actors don't take breaks".

"76% of all ransomware attacks will happen after business hours."

"The majority of organizations that get hit are targeted subsequent times. There's an 80% chance that you will be targeted again within a 90-day period."

"90% of all ransomware attacks are hitting companies with less than $1 billion dollars in revenue."

"These bad actors are really organized crime syndicates. This is not somebody sitting there in their basement doing this as a hobby. They're very well-funded. They're investing in artificial intelligence and machine-learning. They're using the same tools that you as an organization are using."

"Ransomware attacks are really not a one-off situation, we're at a point now where we just have to accept that they are going to happen."

"This is not an IT Problem. This is not a security group problem. This is a business problem. It can only be solved with all parts of the business participating and taking an active role in protecting the organization."

"It's about protecting the revenue, reducing the risk and controlling the cost."

"A successful defense against ransomware means a partnership between technology, people, and process."

**-Paul Furtado, Research Vice President at Gartner**

I had the pleasure of speaking with Paul recently on the phone and he confirmed what I've shared here. CIOs need to rethink this problem. The old approaches simple aren't effective enough anymore. And he reminded me of a fact we all have to face when he said; "Very few CIOS get fired for experiencing a cyber-attack, many get fired for how they respond to one."

**RYAN COTE** is a Chief Information Officer (CIO) with more than 30 years of experience delivering IT-empowered business solutions that drive growth and efficiency for high-performing companies. A veteran of the U.S. Marine Corps, Ryan has an accomplished background working in the Federal government and businesses of all sizes, from small and mid-sized businesses to Fortune 100 companies. From 2019-2021, Ryan was the CIO at the U.S. DOT, where he served as the principal advisor to the Secretary on all IT-related strategy. Prior to the Federal government, Ryan worked at Gartner, Inc., the world's leading IT research and advisory company. As a CIO Executive Partner, Ryan advised fellow CIOs through Gartner's Executive Partners Program. Ryan is also a Gartner Research Board Alumnus. Ryan holds an Executive M.S. in Technology Management from Columbia University and serves on numerous advisory boards.