

EXECUTIVE BRIEF

The Real Cost of Ransomware

Abstract

With attacks growing in sophistication, and cybersecurity budgets and headcounts remaining stagnant, it's important for organizations to understand what's truly at stake in a cyberattack, so that they can properly allocate their resources and prioritize their prevention strategies.

Unfortunately, in cybersecurity, it's often challenging to quantify risk — and some of our most common ways of evaluating risk fall short of capturing the effects of some attacks, particularly ransomware attacks.

Quantifying Risk

Most cybersecurity practitioners are familiar with the "heatmap" matrix commonly used to evaluate cybersecurity risk. On one axis, likelihood proceeds from "rare," "remote" or "very unlikely" to "almost certain," "very likely" or "frequent." Along the other axis, attack impact is ranked with terms like "negligible" and

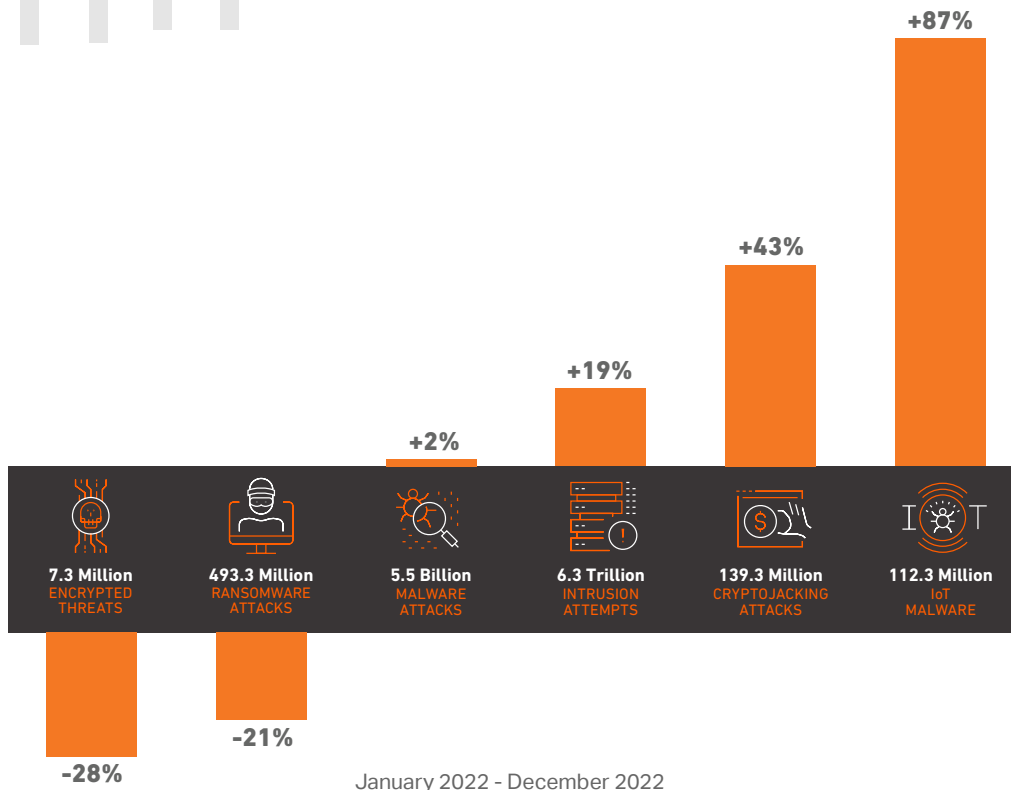
"insignificant" on one end and "catastrophic" or "severe" on the other. Find the point where the axes intersect for whichever sort of incident you're envisioning, and that's your risk ranking.

But while these matrices can be useful tools, they shouldn't form the basis for your cybersecurity decision-making on their own. The context they can provide is valuable, but they aren't capable of adequately capturing the full scope of risks posed by attacks such as ransomware.

How Risky is Ransomware?

In CISA's most recent [Cost of Cyber Incidents report](#), ransomware was only the second-most common loss category for SMBs, lagging significantly behind social engineering. Among large entities, there was only a single ransomware incident among the businesses surveyed, versus 18 for "malware/virus" and 20 for "hacker."

		Impact →				
		NEGLIGIBLE	MINOR	MODERATE	SIGNIFICANT	SEVERE
↑ Likelihood	VERY LIKELY	Low Med	Medium	Med Hi	High	High
	LIKELY	Low	Low Med	Medium	Med Hi	High
	POSSIBLE	Low	Low Med	Medium	Med Hi	Med Hi
	UNLIKELY	Low	Low Med	Low Med	Medium	Med Hi
	VERY UNLIKELY	Low	Low	Low Med	Medium	Medium



January 2022 - December 2022
 Source: The 2023 SonicWall Cyber Threat Report

More recently, [IBM found that](#) 28% of the businesses they surveyed had been victim of a ransomware or “destructive” attack, versus 83% that had experienced more than one data breach. In fact, ransomware made up only 11% of reported incidents — compared with 21% for human error and 24% for IT failures — making it the smallest category aside from “other.”

[SonicWall's own recent data](#) showed ransomware falling by over a fifth in 2022, including a 48% decrease in North America — while almost every other threat type showed an increase.

If severity can be equated to financial impact, the data again seems to suggest ransomware isn't too much of a concern. In the latest IC3 report, the most expensive form of cybercrime type in 2021 was BEC/EAC attacks, which resulted in a \$2,395,953,296 loss — completely eclipsing ransomware's losses of \$49,207,908.

Based on these stats — the same types of stats generally used with risk matrices — it would be tempting to rank ransomware somewhere in the neighborhood of “medium” and deprioritize ransomware preparation. But doing so could prove to be a very costly mistake.

A More Comprehensive View of Ransomware Risk

While historical data is inarguably a valuable tool, security professionals need to ensure they're taking ransomware statistics in context. For example, while data from SonicWall and others show that ransomware was down in 2022 from its halcyon 2021 totals, 2022 still had easily the second-highest volume in the last five years.


And while cybersecurity vendors tend to have a pretty good idea of how much ransomware is going through their own solutions, that doesn't mean that all of these incidents are necessarily being reported.

As a result, there's a growing concern about the scale of underreporting when it comes to ransomware. In a [U.S. Senate Judiciary Committee hearing](#), Deputy Assistant Attorney General Richard Downing said his agency believes that “only about a quarter of ransomware intrusions are actually reported.”

This concern isn't limited to the United States. Across the pond, [an NCSC report](#) released in November 2022 admitted that the impact of ransomware cannot be accurately determined. “The true numbers of ransomware attacks in the UK each year are far higher [than stated], as organizations often do not report the compromises,” the report stated.

The number of incidents isn't the only thing being undercounted, however. Due to the complexity of these attacks, much of the data that exists for ransomware paints an incomplete picture of the costs associated with the attacks that are reported.

For example, the IC3 ransomware total of \$49,207,908 almost seems encouraging compared with loss totals from other threat types. But there's an asterisk: In the fine print at the bottom, the report notes that the ransomware adjusted loss estimate “does not include estimates of lost business, time, wages, files or equipment, or any third-party remediation.”



That's a significant omission, since ransom amounts make up [only about 15%](#) of the total cost of a ransomware attack.

Similarly, while IBM found that 28% of businesses had suffered a ransomware attack — lower than for other threat types — it also found that the cost of a ransomware attack was higher than the overall global average for data breaches (\$4.54 million vs. \$4.35 million). And that's without counting the money spent on the ransom itself, which currently [averages about \\$2.2 million](#).

But even taking these things into account, we still don't have a complete picture of ransomware risk. In addition to any ransom paid and the expenses that almost all ransomware victims will face — such as lost business, wages, files and equipment and third-party remediation — there are a number of other possible outcomes that could take any ransomware attack from “bad” to “catastrophic.”

What's the Worst That Could Happen?

While we commonly refer to them as “ransomware attacks,” ransomware is best thought of less as an isolated incident, and more as a series of potential chain reactions. “Lucky” victims might pay the ransom and get a valid decryption key or quickly rebuild with current and intact backups, and that will be the end of it. But as ransomware gangs become both more creative and more ruthless, this is less and less likely to be the case.

Here are just some of the additional concerns in the aftermath of a ransomware attack that should be calculated as part of a comprehensive risk assessment:

Broken/Incomplete Decryptors

Despite what ransomware operators claim, [paying a ransom is no guarantee](#) that files will actually be decrypted. It isn't at all rare for the decryption key to be granted, only for the victim to find it didn't decrypt the data entirely ... or at all. According to a survey by research and marketing firm CyberEdge Group, [nearly 1 in 5](#) ransomware victims surveyed paid the ransom and still lost all their data for good. And since cybercriminals don't exactly operate on a “satisfaction or your money back” policy, these companies are out the total ransom amount and the cost of completely rebuilding.

Downtime

On average, organizations experience [nearly three weeks](#) of downtime following a successful ransomware attack. This downtime can have a significant impact on earnings: in the United States, the economic cost of ransomware amounted to more than \$159 billion in downtime alone.

Double and Triple Extortion

Sometimes a ransomware attack is just a ransomware attack ... but not usually. [Nearly two-thirds](#) of today's ransomware attacks are also data exfiltration operations, an increase of 106% from just five years ago. And while having sensitive data

stolen in a double extortion incident is already a catastrophe, an increasing number of cybercriminals aren't stopping there.

The past two years have seen an increase in the use of triple extortion techniques. In these attacks, cybercriminals not only threaten to release sensitive data — they also filter through it to find customers, patients, stakeholders and anyone else who might have something to lose from that data becoming public, and demand a ransom from them, too.

Repeat Attacks

In spite of promises to the contrary, paying a ransom offers no guarantee that criminals will actually delete the data that they've already stolen. And the fact that an organization has already shown a willingness to pay makes them an even more attractive target. [According to ZDNet](#), roughly eight in 10 organizations that paid ransom demands were subsequently attacked again, with nearly half of these victims saying they believe the second attack was perpetrated by the same criminals as the first.

Lawsuits

Due to the sorts of data often exfiltrated in ransomware incidents, attack targets sometimes find they're also the target of lawsuits filed by one or more affected parties. [Rackspace](#), [Canon](#), [Epiq Systems](#), [TransLink](#), [US Fertility](#) and [Scripps Health](#) are just some of the companies that have been faced with class-action lawsuits in the aftermath of a ransomware attack.

Reputation Damage

Even organizations that aren't taken to court following a ransomware incident often find themselves judged in the court of public opinion. And unlike costs such as forensic investigation and disaster recovery, cyber insurance may not cover all — or any — of the costs stemming from repairing your organization's reputation, such as running ads, purchasing credit monitoring for thousands (or millions) of affected individuals, and other efforts to regain trust and retain business.

Regulatory Fines

In cases where exfiltrated data includes certain types of personally identifiable information, such as financial and PCI (Payment Card Industry) data or medical records and other health information subject to HIPAA, organizations may face large regulatory fines.

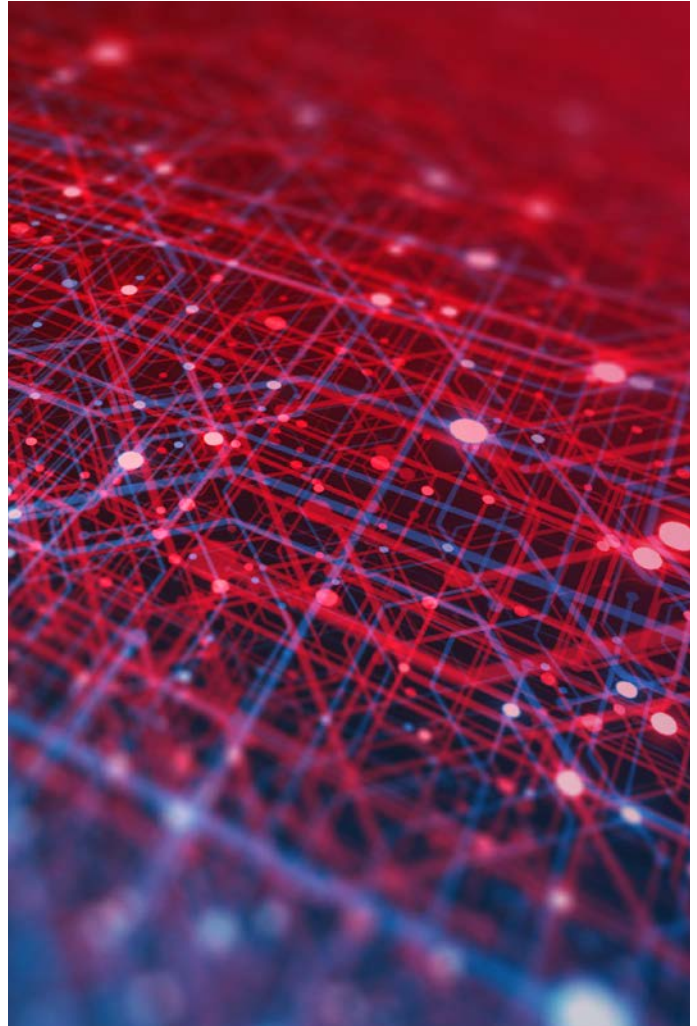
The Power of Preventive Measures

While the risk of ransomware might be bigger than many organizations realize, the good news is that there's plenty of measures that can be taken to help stop these attacks.

- **Update:** Whenever possible, automate the tracking and enumeration of vulnerabilities on applications and devices on your network. Patch early and often.

- **Upgrade:** The older an operating system gets, the more malware and other threats are created to target them. Retire any software or hardware that is obsolete or no longer supported by the vendor.
- **Duplicate:** All important data [should be backed up](#) to a place inaccessible by attackers. Having adequate and up-to-date backups on hand significantly eases recovery in the event of a ransomware attack.
- **Educate:** A staggering 91% of all cyberattacks start with someone [opening a phishing email](#). Teach employees to be wary any time they receive an email, particularly one with an attachment or link.
- **Test:** Responsiveness measures aren't "set it and forget it." Check to see if your business continuity plan works and is up to date. Determine how long it takes to restore from a backup (and make sure your backups are being updated regularly). Verify that you have isolated, air-gapped domain controllers.
- **Safeguard:** The above steps are "best practices" and not "universal practices" for a reason. If any are allowed to lapse — or new methods are found to circumvent them — organizations will need a strong last line of defense. An [advanced, multi-layer platform](#) that includes endpoint security, next-gen firewall services, email security and secure mobile access can work to eliminate blind spots and eradicate both known and unknown threats.

While the information here can help organizations make more fully informed decisions, it's ultimately up to each business to determine what their personal risk — and risk tolerance — to be. By adopting a proactive stance, organizations can lower their risk of attack while increasing their ability to respond to and recover from an attack if it does occur.



Note: SonicWall threat data cited is the 2023 SonicWall Cyber Threat Report.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
 1033 McCarthy Boulevard | Milpitas, CA 95035
 Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

© 2023 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.