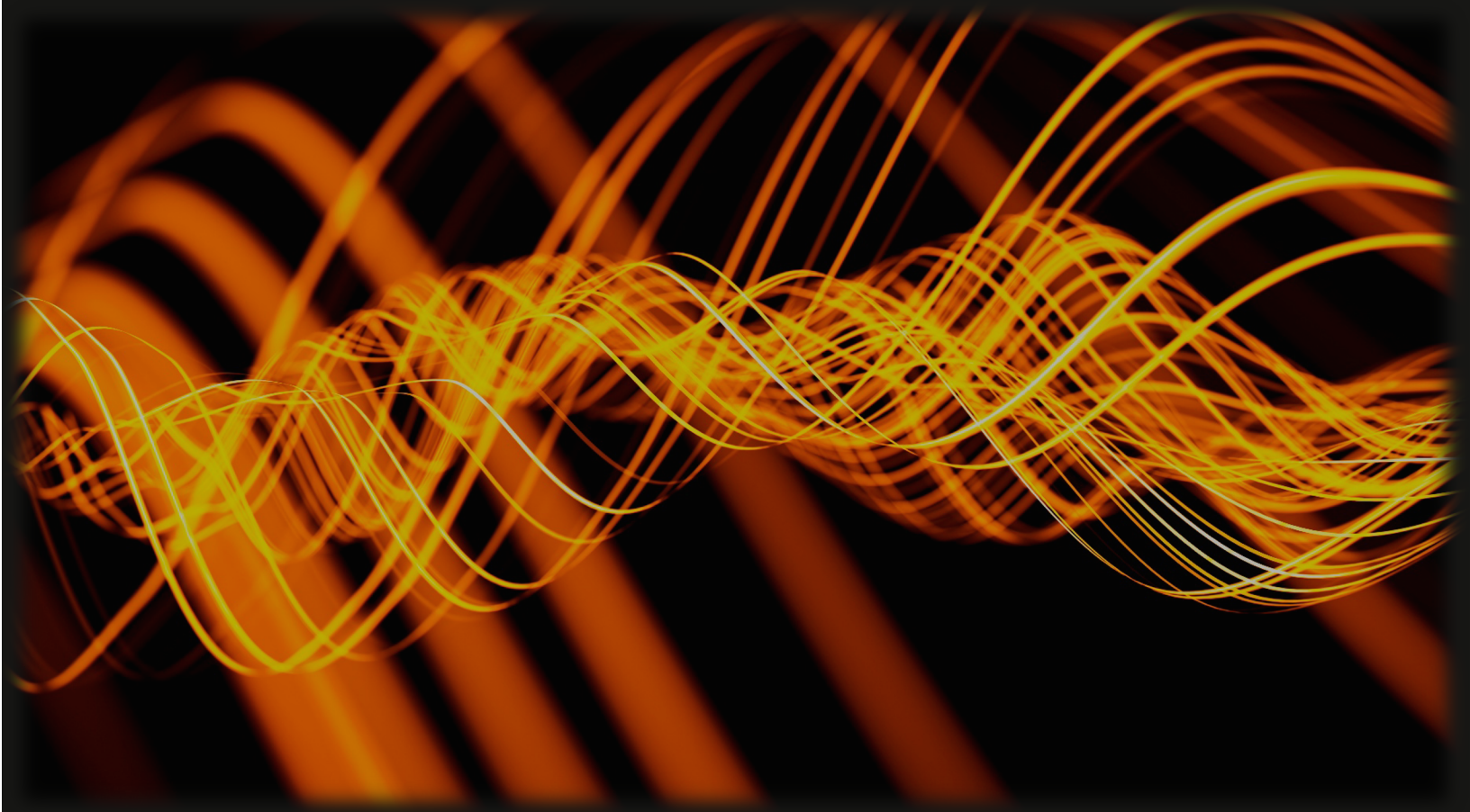
Ransomware in the Supply Chain: Seven Lessons from 11 Years of Attacks

Data-driven insights to reduce ransomware exposure and secure your supply chain

THOUGHTLEADERSHIPPAPER
June 2026



Contents

Introduction

Ransomware has evolved from isolated criminal activity into one of the defining operational risks facing modern organizations. What once targeted individual systems and demanded hundreds of dollars now routinely disrupts hospitals, manufacturers, schools, governments, retailers, and critical infrastructure with consequences that cascade well beyond the immediate victim.

The challenge facing organizations today is not simply defending their own networks. Modern enterprises operate through complex ecosystems of suppliers, technology providers, partners, and service organizations that collectively determine operational resilience. A ransomware event affecting a single third party can shut down operations, delay payments, halt customer services, disrupt healthcare delivery, or create downstream impacts across entire supply chains.

Mastercard Cybersecurity researchers cataloged and analyzed 8,315 publicly reported ransomware events occurring between 2015 and 2025. These incidents reveal a clear reality: ransomware is no longer solely an endpoint security problem or an IT problem—it is a business continuity and supply-chain resilience challenge.

The data also reveals something encouraging; ransomware outcomes are not random. Organizations with stronger cybersecurity hygiene consistently experience materially lower frequencies of damaging events. The patterns are measurable, and risk can be identified before disruption occurs.

This report distills seven key lessons from eleven years of ransomware activity. The objective is not simply to understand what happened, but to help organizations answer critical questions:

- Which suppliers introduce the greatest operational risk?
- Which cybersecurity indicators most strongly correlate with damaging outcomes?
- How can organizations scale risk management across increasingly complex ecosystems?
- What actions improve resilience before an incident occurs?

The organizations that manage ransomware risk most effectively will be the ones using intelligence and observable risk signals to identify weaknesses early, prioritize action, and strengthen resilience across both their enterprise and their supply chain.

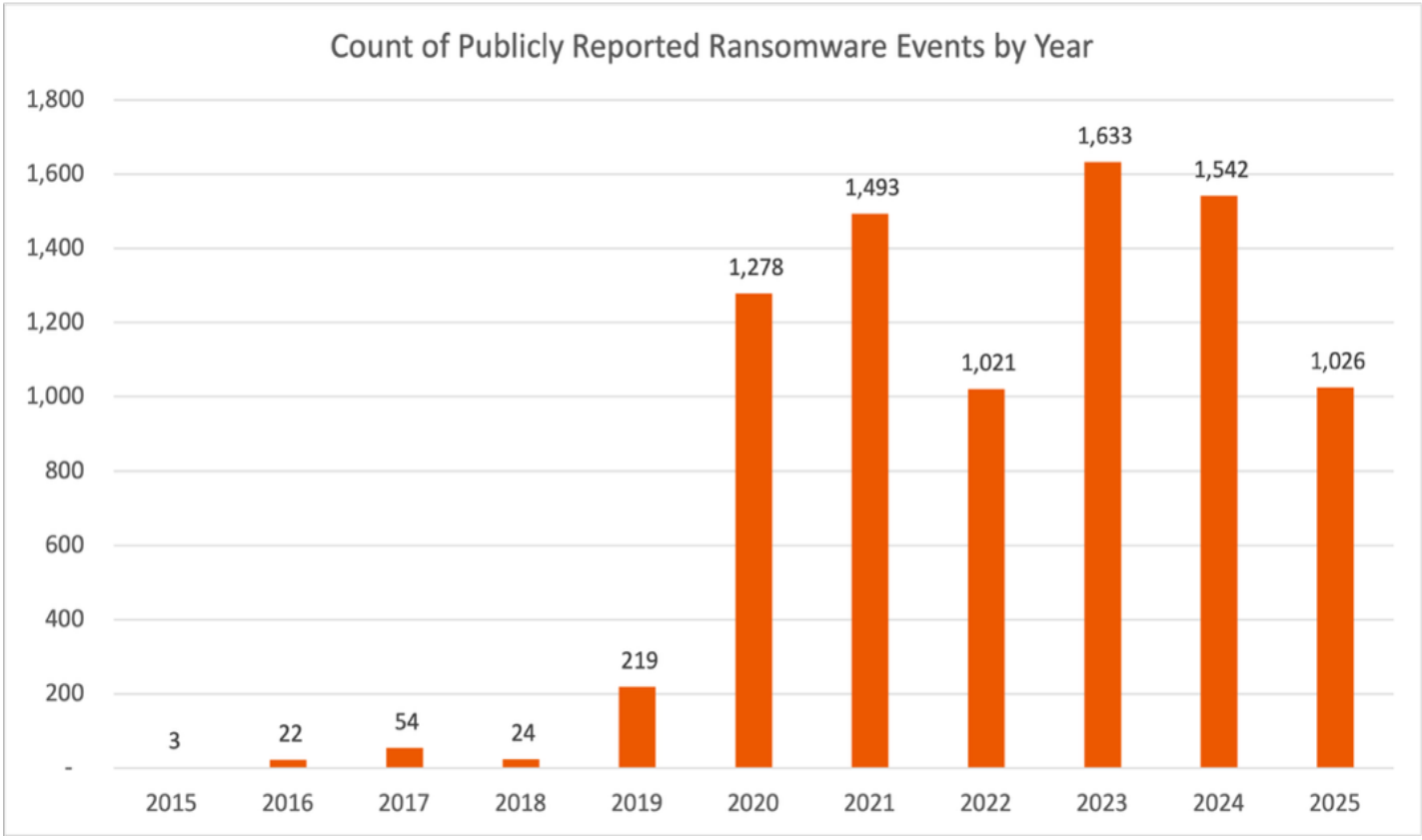
The Study

RiskRecon by Mastercard continuously monitors the cybersecurity hygiene of over fifteen million organizations, spanning all industries and nearly all parts of the globe. For this study, we selected 263,000 companies for which RiskRecon maintains human-supervised, continuous cybersecurity assessments on behalf of its customers which have relationships that pose particularly high risks with these organizations. Beyond continuously analyzing the cybersecurity configurations of each company's internet-facing systems and related signal intelligence, RiskRecon analysts catalog breach events occurring within each company.

Events

RiskRecon cataloged and studied 8,315 publicly reported ransomware events that occurred between January 2015 and December 2025. These events were identified through internet keyword searches, monitoring of event disclosure sites, dark web and open web ransomware sites, local and international news sites, and 8-K SEC filings.

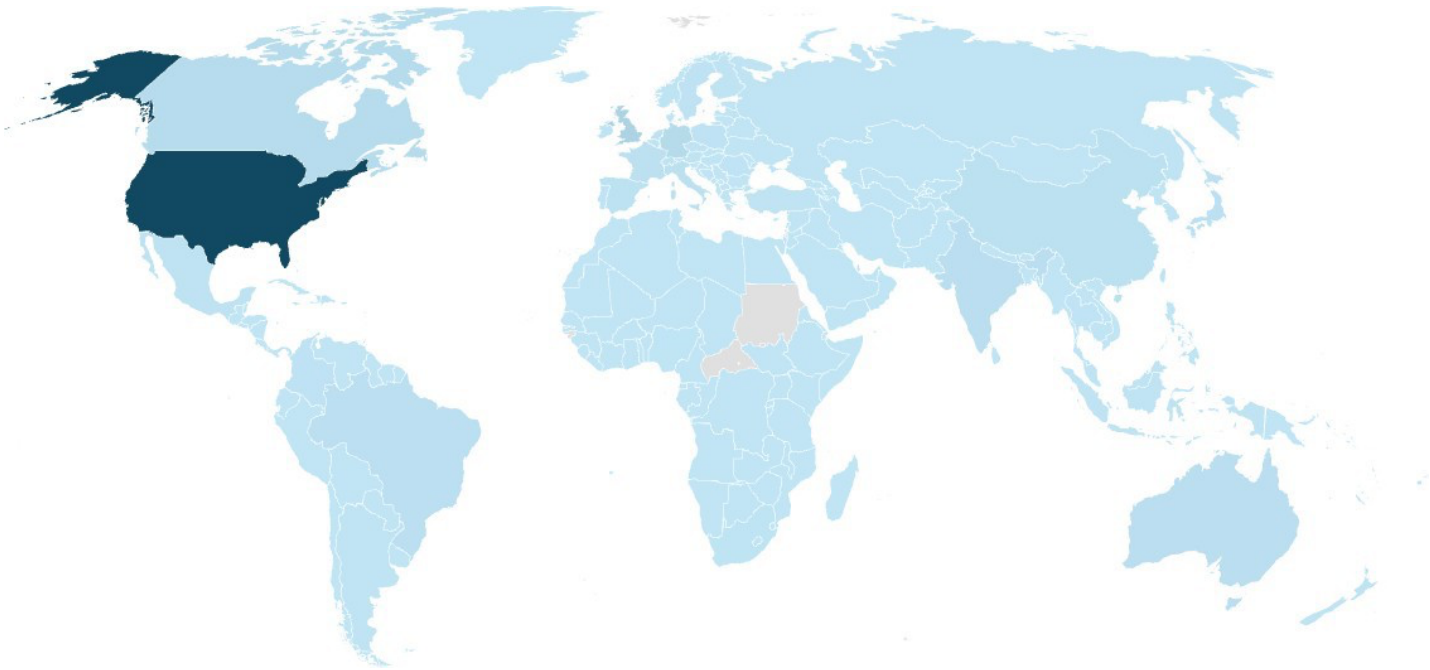
For purposes of this study, a ransomware event is defined as any cybersecurity breach event in which data is exfiltrated from the organization and/or one or more systems are encrypted that meaningfully impact operations and restoration of the systems or promise to not disclose data is made contingent on payment of a ransom.



Determining the exact number of ransomware events occurring across a large and distant population is difficult. Many reported ransomware events are not real. While our research spanned hundreds of dark, deep, and open web sources, we limited our cataloged events to those we considered to be from reliable sources. Further challenging the study of ransomware events, disclosures are biased and unevenly reported. Not all companies publicly report all breach events; it varies based on factors such as geography, industry, and country-specific reporting requirements. That said, we have done our best with the data available.

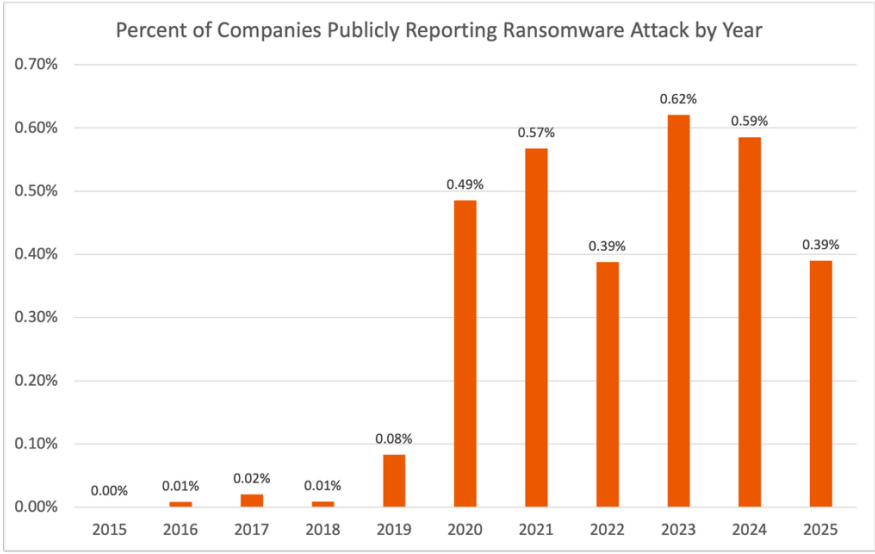
Geography

The study encompasses companies with primary centers of operation in 245 countries and territories. Most of the organizations are based in the U.S., accounting for 55% of the population. The United Kingdom accounts for 7%, Germany for 4%, and Canada for 3%. Australia, India, China, and Brazil, France, Japan, and Spain each account for between 1% and 2%.

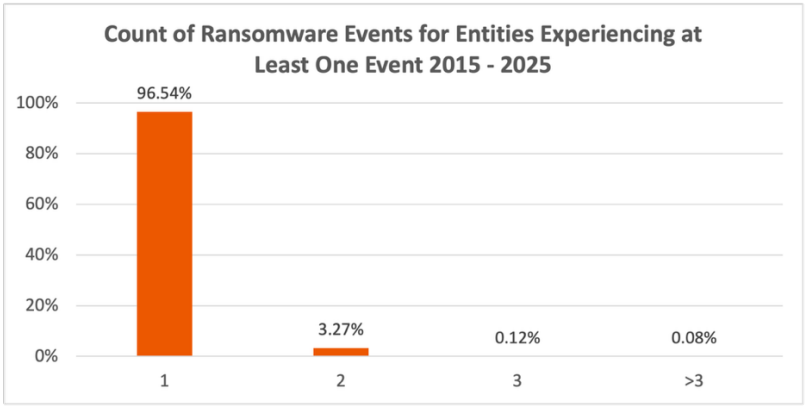


Lesson 1: About one in two hundred chances

Over the last five years, about one of every two hundred organizations (0.51%) publicly reported falling victim to a ransomware attack each year. Since 2015, 3.1% of organizations have suffered at least one impactful ransomware attack. The annual rate has grown from near zero in 2015 when only two of the organizations were compromised to a 10-year high in 2023 of 0.62% (62 of every 1,000 organizations).



It is rare that an organization succumbs to more than one major ransomware attack. Since 2015, 3.1% of the organizations in the study have been hit by a damaging ransomware attack. Of those, 3.5% have been victimized more than once – a probability of 0.1% (3.2% x 3.5%) in the 11-year span. The Government of the Philippines was the unfortunate victim of five ransomware attacks, with separate attacks hitting departments covering science and technology, education, health insurance, and migrant workers. The governments of Costa Rica, Mexico and Brazil had four events.

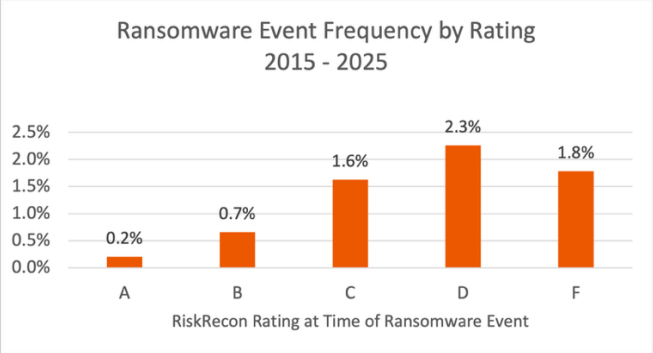


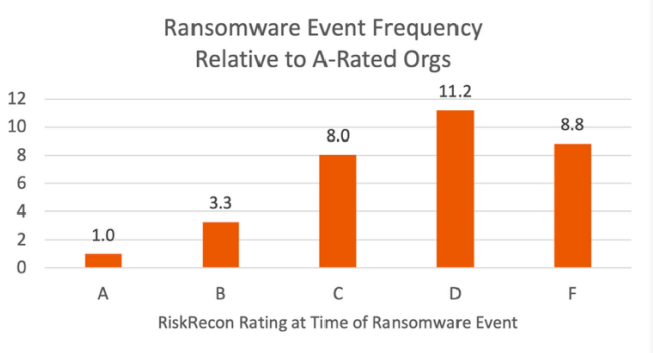
One in 200 chances per year seems to be low odds but is very significant when considering protecting a supply chain. Larger companies that have hundreds or thousands of suppliers could be dealing with five, ten, or more ransomware shocks to their supply chain each year.

Lesson 2: Good cybersecurity hygiene pays well

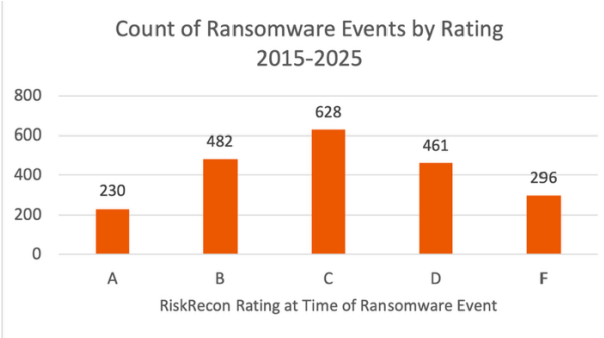
RiskRecon had visibility into the cybersecurity hygiene of 2,097 ransomware attack victim organizations at the time of the incident. Based on this data, those with very poor cybersecurity hygiene, rated by RiskRecon as D or F, experienced a 10.1x higher frequency of ransomware events compared to A-rated organizations, which RiskRecon observes as having very clean hygiene. Since 2015, only 0.2% of A-rated companies and 0.7% of B-rated companies suffered a ransomware event. In comparison, 2.3% of D and 1.8% of F-rated companies have had a ransomware event from 2015 through 2025.

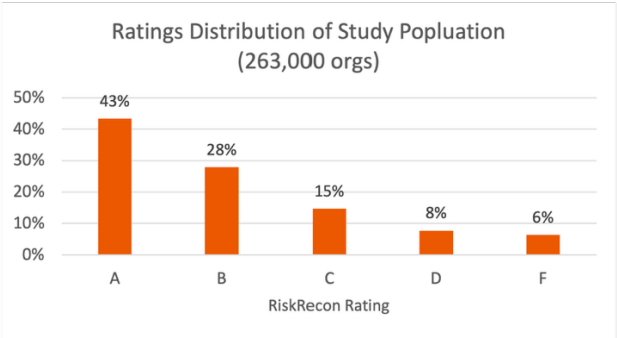
Organizations with good cybersecurity hygiene have
10.1x lower
frequency of ransomware events





Lest one think that the larger populations of A and B rated organizations are skewing the correlation, across the population of 263,000 entities A-rated organizations have a 7.1 times larger population than F-rated while having 28% fewer ransomware events. The graphs of event counts by rating and the rating distribution of the organizations are shown below.





The cybersecurity conditions underlying the RiskRecon rating reveal just how poor the cybersecurity hygiene is of companies, on average, that fall victim to a material ransomware attack. In comparison with the general population, those that succumb to ransomware, on average, have:

- 15.3 times more high and critical severity software vulnerabilities in their internet facing systems.
- 12.5 times more unsafe network services exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.
- 10.1 times higher rate of application security issues such as not implementing encryption in systems that collect sensitive data and application platform administration interfaces exposed to the internet

with single-factor authentication.

- 11.5 times higher frequency of encryption configuration issues in high value systems that collect and transmit sensitive data.

	Average Issue Count		
	Ransomware Victim	**General Population**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	12.2	0.8	15.3x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	20.0	1.6	12.5x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	20.2	2.0	10.1x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	35.6	3.1	11.5x higher

Table: *Comparison of count of security issues in internet-facing systems surrounding day of ransomware detonation*

Ignoring issue counts and just looking at the percent of companies with at least one issue in their internet facing systems, the ransomware victim group again stands out as having very poor hygiene in comparison to the general population.

	Percent with at Least One Issue		
	Ransomware Victim	**General Population**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	46%	15%	3.1x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	46%	18%	2.6x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	55%	30%	1.8x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	60%	28%	2.1x higher

Table: *Comparison of percent of organizations with at least one issue in their internet-facing systems*

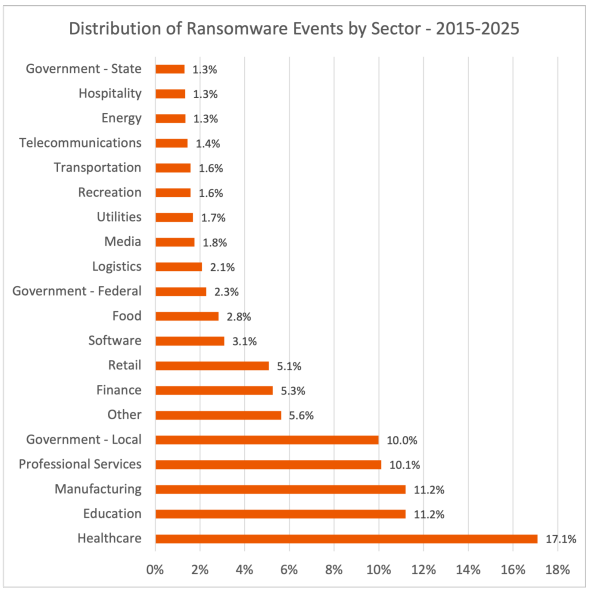
Why such a strong correlation? Organizations that have poor security hygiene in their external surface not only provide easy initial entry vectors, but they are also less likely to have strong internal defenses that are necessary to resist ransomware gangs. Conversely, organizations that demonstrate very clean hygiene in their externally observable systems and signals do not offer as many initial entry vectors and are more likely to maintain strong internal defenses. No guarantee, but more likely.

The lesson for supply chain risk management? Do business with organizations that have good cybersecurity hygiene; they have upwards of 10x fewer ransomware events than those with poor hygiene.

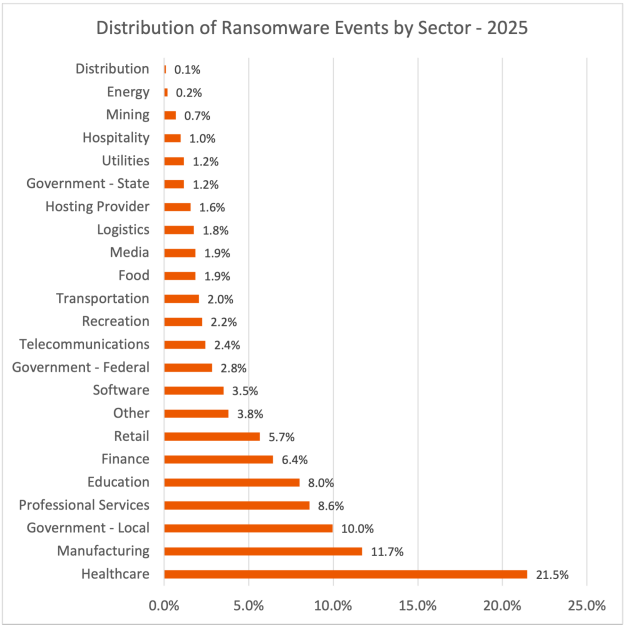
Lesson 3: Criminals are targeting every sector

Across the 8,315 ransomware events occurring from 2015 to 2025, criminals disrupted the operations of organizations across 81 different sectors. In 2015, just two industries were hit: utilities and police. As of 2025, the victim list has expanded to include casinos, hotels, local fire and police departments, agriculture, churches, and cruise lines. Even veterinary clinics.

Unfortunately for society, healthcare providers have been hit the most, accounting for 17.1% of all ransomware events, rendering hospitals and clinics inoperable in geographies ranging from Japan to Germany. Education, spanning K-12 and universities, has struggled to keep control of their systems, accounting for 11.2% of ransomware events. Manufacturing also came in at 11.2%, likely due to their reliance on IoT devices. Professional services (10.1%), and local governments (10.0%) also have taken heavy hits.



Focusing on attacks occurring in 2025, healthcare bore even more of the pressure accounting for 21.5% of the publicly reported ransomware attacks.

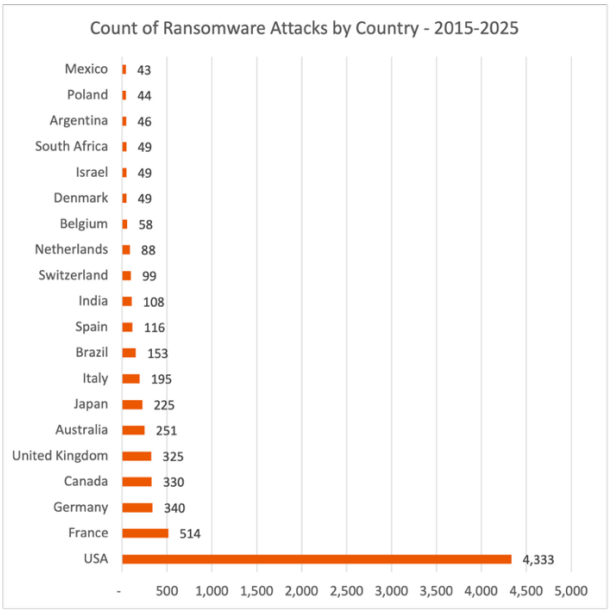


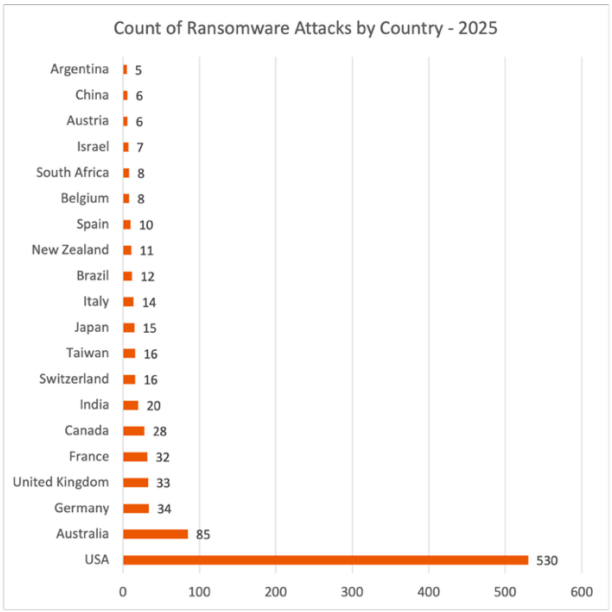
Every organization is a candidate for destruction at the hands of cybercrime groups. Each vendor and partner is a possible target. Know the ones you are operationally dependent on. Those suppliers that were previously rated as low inherent risk due to lack of data or transaction sensitivity might be high or critical when examined through the lens of operational dependency.

Lesson 4: Criminals are hitting every geography

Criminals are striking organizations in every major geography. RiskRecon cataloged ransomware events in 137 of the 245 countries and territories included in the study. While the bulk of the attacks follow the level of economic activity, some reached remote areas such as Vanuatu, North Macedonia, and Nauru. In the case of Vanuatu, the October 2022 attack shut down government systems for over a month, forcing agency personnel to resort to typewriters, pen and paper, and Gmail to continue operations.

Since 2015, we tallied 4,333 successful attacks against US-based organizations. France came in second at 514, followed by Germany at 340, Canada at 330 and the United Kingdom at 325. China and Russia, having the second and ninth largest economies, are notably absent.



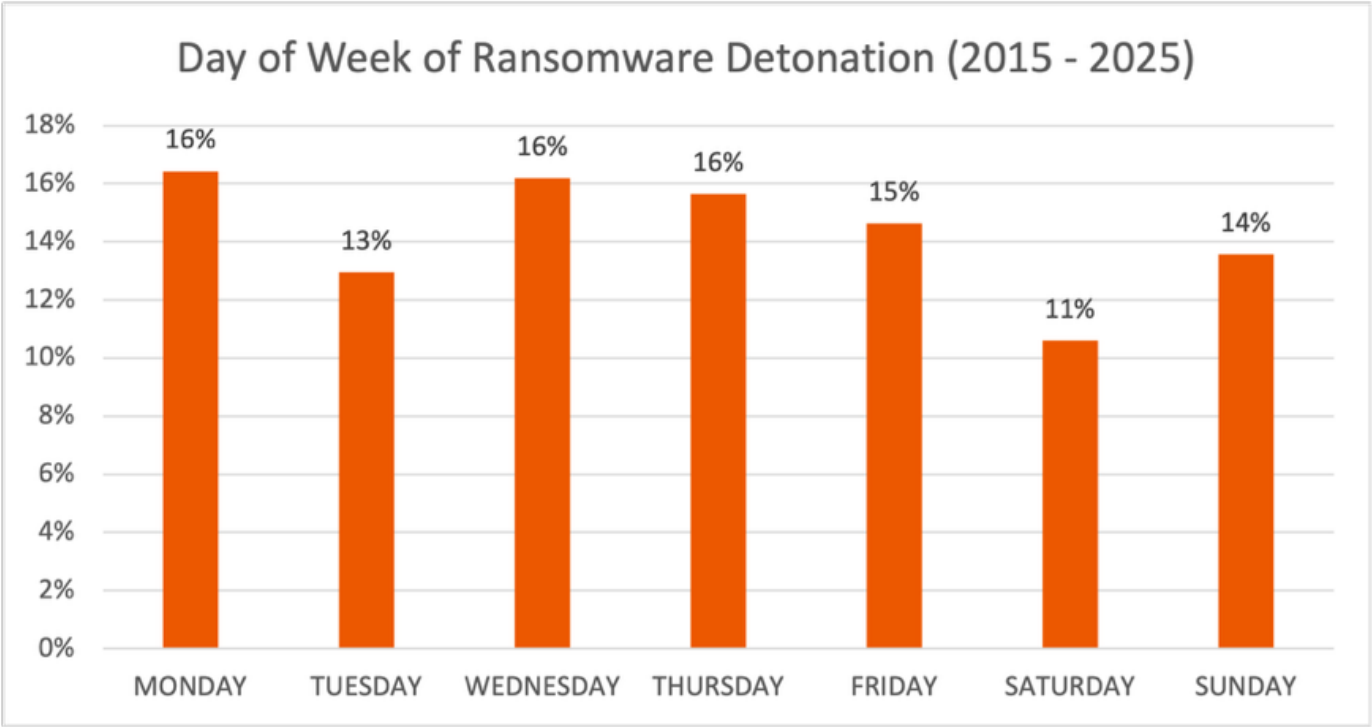


Looking just at 2025, Australia jumped into second spot with 85 ransomware events. The Land Down Under saw attacks against organizations ranging from Qantas airlines to Nina's Jewelry, a small family business.

It is common to have supply chains spread across the world. They may be distant geographically, but they are all next door on the internet. And just because there aren't many breach events being reported out of certain countries doesn't mean that breach events aren't happening. It is likely because there is a lack of cybersecurity regulations and reporting requirements. Suppliers in regions with weak regulations may require more governance than others.

Lesson 5: 24x7 security operations is essential

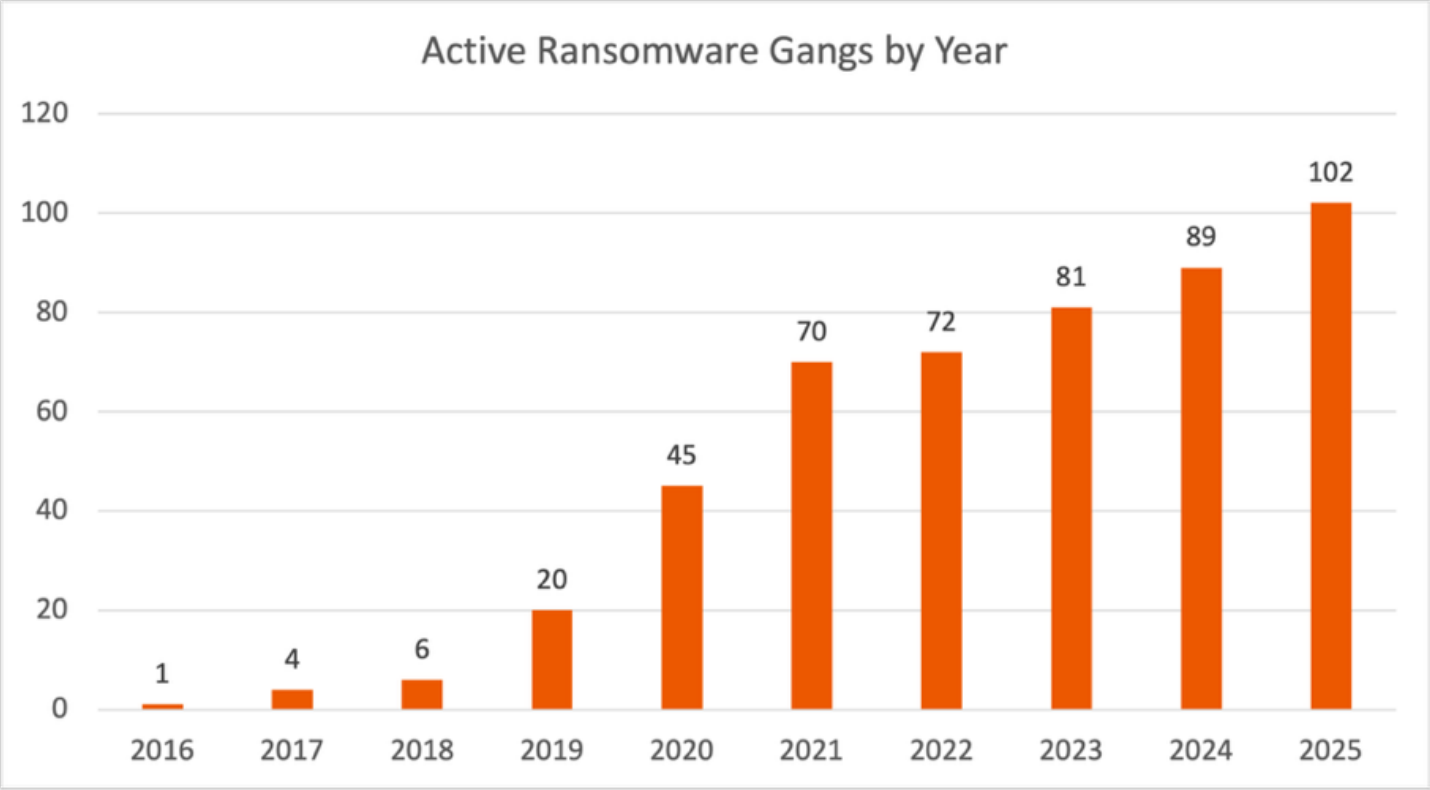
This section is short, but important. Based on the date of initial compromise reported by companies across the 8,315 events, criminals are detonating ransomware seven days a week, with no day of the week having less than 10% of the total events.



Ensure that your operationally important suppliers have 24x7 IT and security operations every day of the year, including holidays. Rapid response to a ransomware event is essential to limiting damage and getting on with recovering systems and operations.

Lesson 6: Settle in for the long-haul

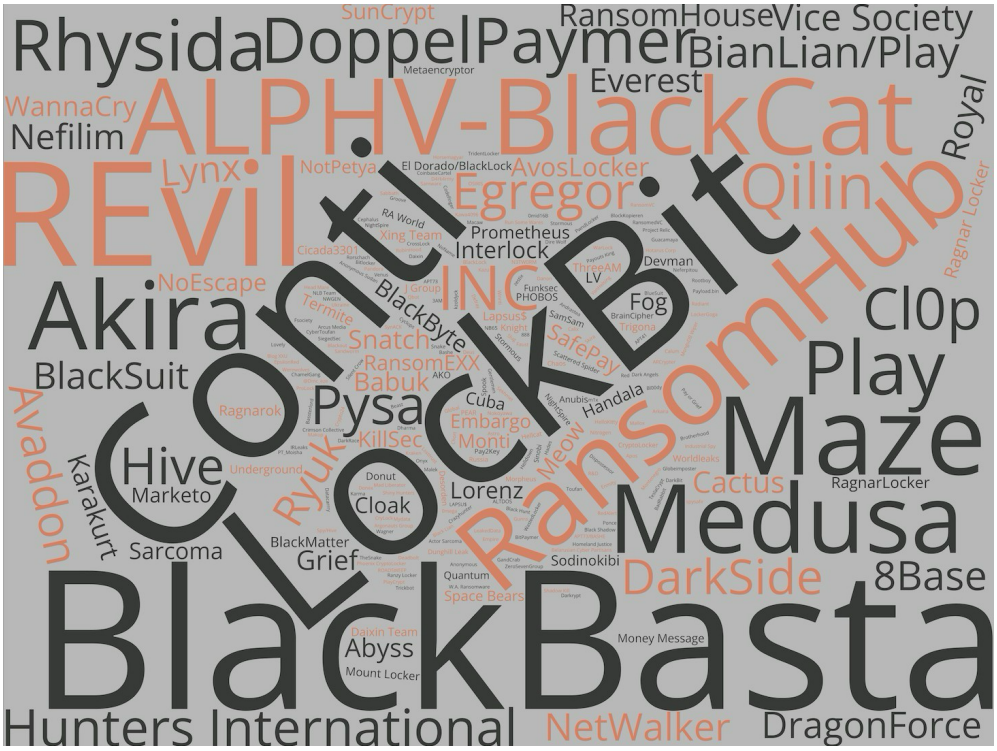
The ransomware threat is here to stay because it is highly profitable for criminals and it is a high-impact munition for nation states. In 2019, criminals learned that organizations were willing to pay big money to restore system operations. The very next year the number of ransomware attacks jumped nearly 6x and the number of gangs doubled.



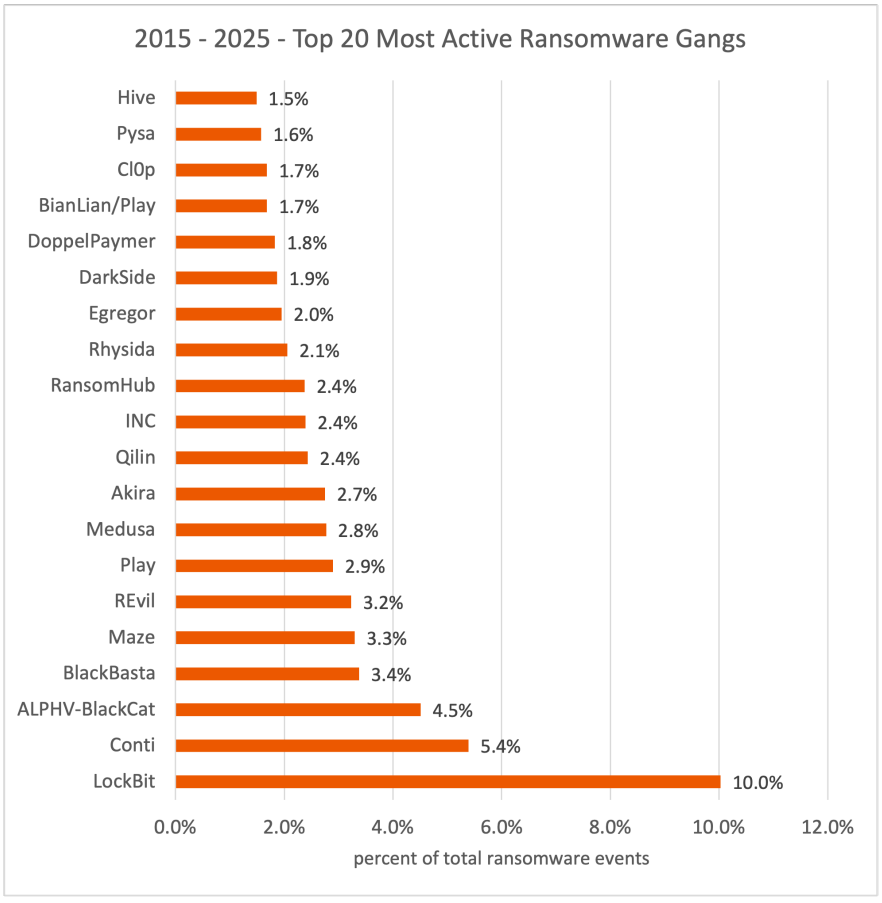
Follow the money here. The Houlton Maine police department paid $588 in 2015 to restore their systems. Hollywood Presbyterian Medical Center set the high mark for 2016, coming in at $17,000. And the government of Montgomery County, Alabama paid nearly $50,000 in 2017. By 2018 six-figure ransomware payments were common. The season of big game hunting had officially started.

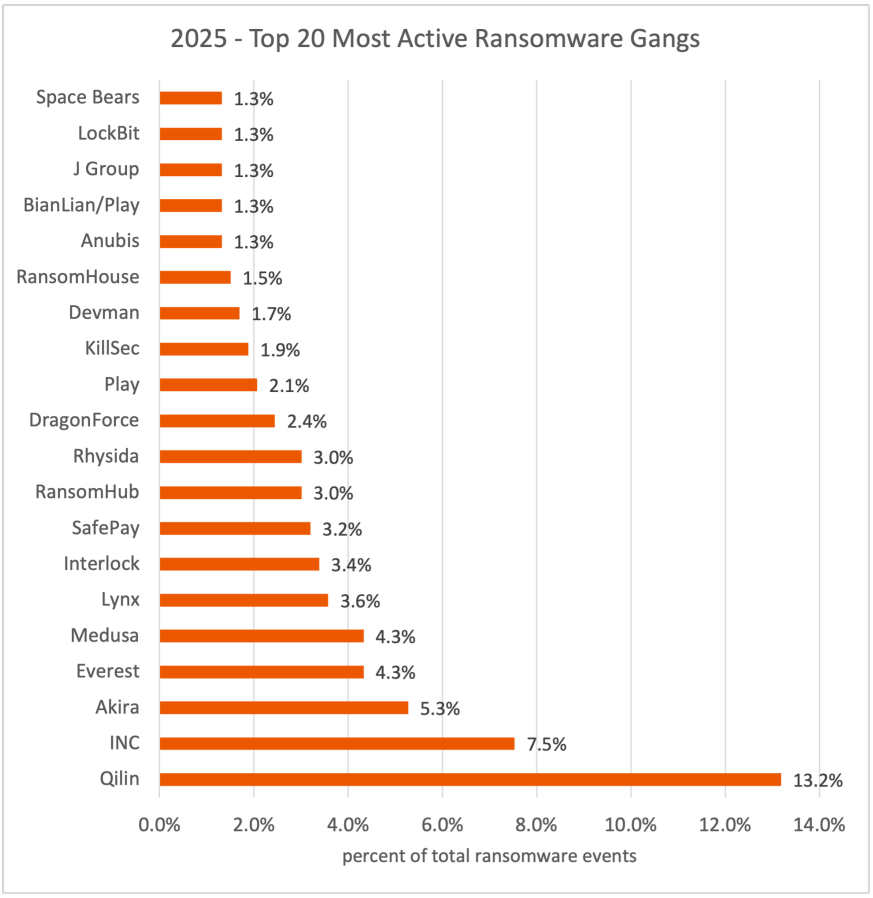
As profits grew, so did specialization of labor, making it easy for new criminals to enter the scene. Initial Access Brokers (IABs) took hold and started selling ready enterprise access, allowing ransomware operators to skip the time-consuming initial breach phase. This, coupled with the licensing of ransomware code, 24x7 support included, transformed cybercrime from requiring deep and broad expertise to Ransomware-as-a-Service (RaaS). Simply license the software, buy the access, then detonate the ransomware on the right systems.

This "easy business model" has driven a dramatic growth in the number of ransomware variants and operators. In 2017 there were only four hitting the companies in this study – WannaCry, NotPetya, SamSam, and MongoDB Wiper. Since 2015, just within this study population, we identified 277 ransomware gangs, with 102 successfully exploiting organizations in 2025 alone. New gangs in 2025 included NightSpire, @dmc_eze, and Cephalus, the last of which debuted with an attack on the town of Vienna, Virginia.



Lockbit has been the most active variant, accounting for 10% of all cataloged events, first emerging on the public radar in 2020 in an attack against PTI News, an India-based media company. Cl0p has been the most long-lived group, first showing up in this study population in October 2019 in an attack against the University of Antwerp and remaining active through 2025, closing out the year in November with an attack on a Korea-based airline catering service.





So, what does it mean to settle in for the long haul in the battle against ransomware in the supply chain? Update your supplier assessment criteria and related procedures to place added emphasis on controls that are critically important for reliability and resilience in the face of ransomware.

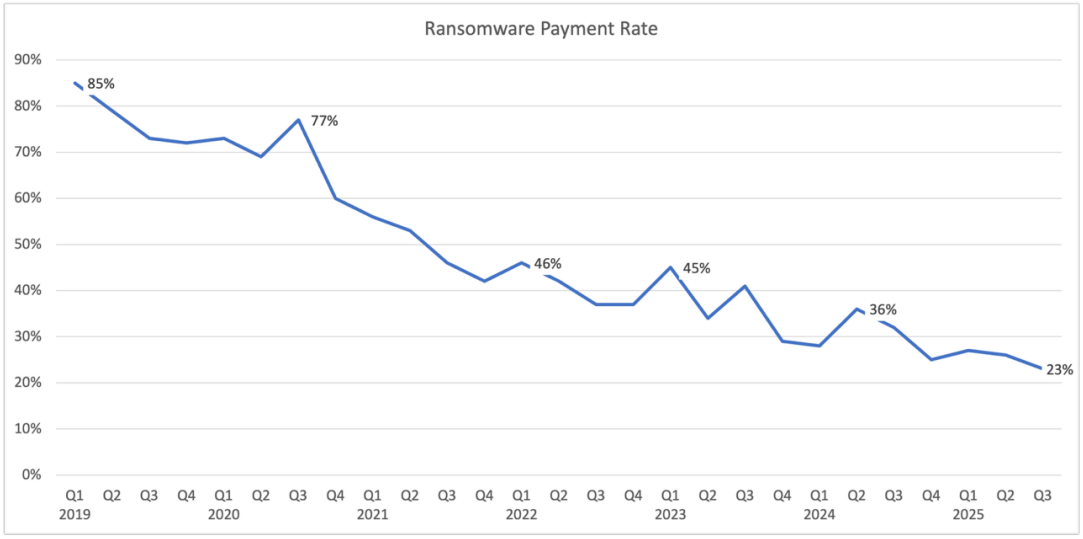
To that end, the US Cybersecurity and Infrastructure Security Agency #StopRansomware Guide has great recommendations (https://www.cisa.gov/resources-tools/resources/stopransomware-guide). The UK's National Cyber Security Centre also has valuable recommendations (https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks)

Lesson 7: There are reasons to be optimistic

There are three clear reasons to be optimistic in the fight against ransomware.

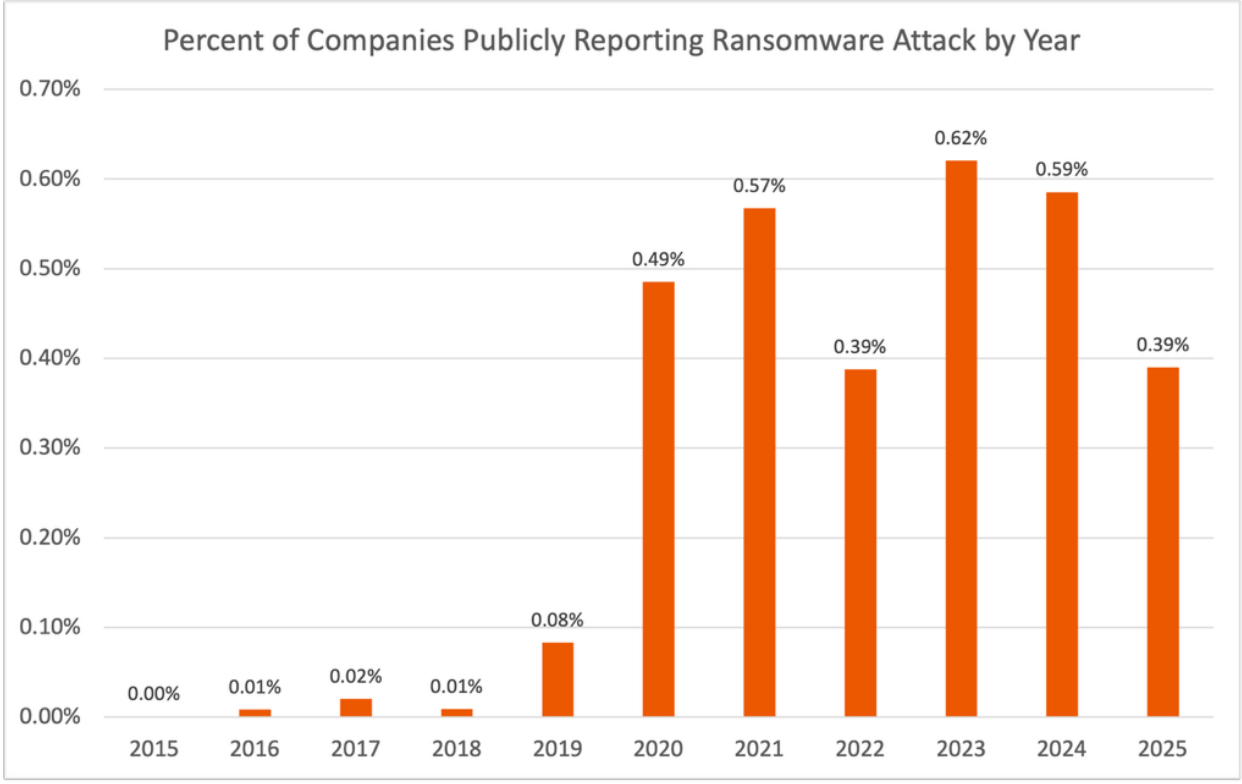
1) The percent of organizations paying ransom is at an all-time low.
2) The number of successful attacks is at a five-year low.
3) Good cybersecurity hygiene is paying off.

Organizations are resolving most ransomware attacks without paying the criminals. According to Coveware, a cyber extortion incident response company, the percentage of ransomware events that involve payment of the ransomware is an all-time low, dropping from a high of 85% to 23% in Q3 2025.[1] While the details of the decrease in payments is not known, it likely means that organizations are more resilient to ransomware attacks. Also, fewer payments mean less money for criminals. Good!

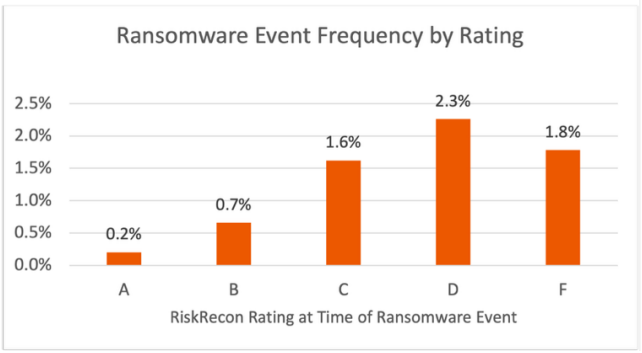


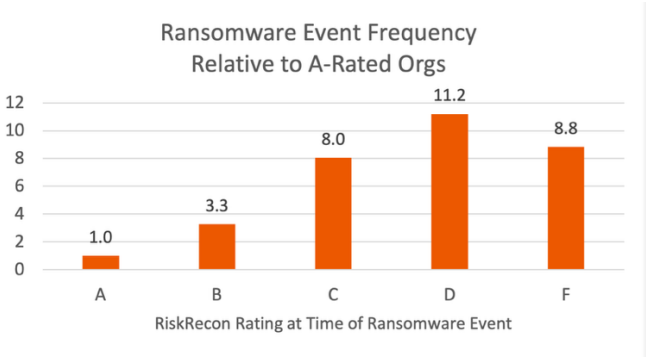
The second reason to be optimistic is that, at least based on this large study population, the annual frequency of companies succumbing to ransomware attacks is decreasing. We went from a high in 2024 of 0.62% of all companies ransomed to 0.39% in 2025.

[1] https://www.coveware.com/blog/2025/7/21/targeted-social-engineering-is-en-vogue-as-ransom-payment-sizes-increase



Last, it is still the case that good cybersecurity hygiene pays well. While companies with good cybersecurity do still succumb to criminals, they fall at a much lower frequency than those that have poor hygiene. And it isn't a trivial amount. Our data shows a 10x lower frequency! Be a business with good cybersecurity hygiene. Do business with organizations that have good cybersecurity hygiene. You will have much better risk outcomes.





Conclusion

Ransomware is no longer an isolated cybersecurity event. It has become an operational and ecosystem risk capable of disrupting business continuity far beyond the boundaries of a single organization.

The findings from this study point toward several practical actions for security and risk leaders:

1. Treat supply chain risk as a resilience problem, not just a compliance exercise
Traditional approaches built around annual questionnaires and static assessments are no longer sufficient. Organizations need continuous visibility into the evolving security posture of the companies they depend upon.

2. Prioritize operationally critical suppliers first
Not every vendor creates equal risk. Focus attention on suppliers whose disruption would materially impact business operations, customer experience, or revenue generation.

3. Use measurable cybersecurity signals to drive decisions
The evidence in this study is clear: organizations with poor cybersecurity hygiene experience dramatically higher frequencies of ransomware events. External indicators such as software vulnerabilities, unsafe services, application security weaknesses, and encryption issues provide actionable signals for predicting risk.

4. Move from reactive assessments to intelligence-driven risk management
The scale and speed of modern supply chains make manual processes difficult to sustain. Security teams need the ability to continuously identify risk, prioritize remediation, and understand where exposure is changing across interconnected ecosystems.

5. Help strengthen the broader ecosystem
No organization exists in isolation. Improving resilience across suppliers, partners, and critical service providers ultimately improves resilience within your own organization.

The encouraging finding from this study is that ransomware outcomes are not inevitable. Organizations with strong cybersecurity hygiene and mature risk management practices consistently experience better outcomes.

You can outsource infrastructure, applications, and services. You cannot outsource accountability for risk. The organizations best prepared for the future will be those that continuously measure, understand, and strengthen resilience across the ecosystems they depend upon.

Free Trial: Understand the Risks Hidden Across Your Supply Chain

This study found that organizations with poor cybersecurity hygiene experience dramatically higher rates of ransomware events. The challenge for most organizations is not understanding whether risk exists—it is identifying where it exists across hundreds or thousands of suppliers.

With RiskRecon, you can gain visibility into the cybersecurity posture of your digital supply chain and identify suppliers that may introduce elevated risk before disruption occurs.

Start with a complimentary Know Your Portfolio assessment and:

- ✓ Assess the cyber hygiene of up to 50 suppliers in your digital ecosystem
- ✓ Identify vendors with elevated risk exposure and poor security practices
- ✓ Understand security issues tied to ransomware risk outcomes
- ✓ Prioritize remediation and engagement efforts based on actionable intelligence
- ✓ Gain immediate visibility into supply chain risk trends

Start your free trial here!

About Mastercard Cybersecurity

Mastercard Cybersecurity is helping organizations secure their infrastructure, applications, third parties, and global supply chains by providing deep visibility into risk across internal systems and external relationships. Through unique threat intelligence, cyber risk insights, and multi-layered, cloud-based defense technologies, Mastercard helps organizations and consumers address risk in real-time, enhancing resilience against today's most sophisticated cyberattacks.
