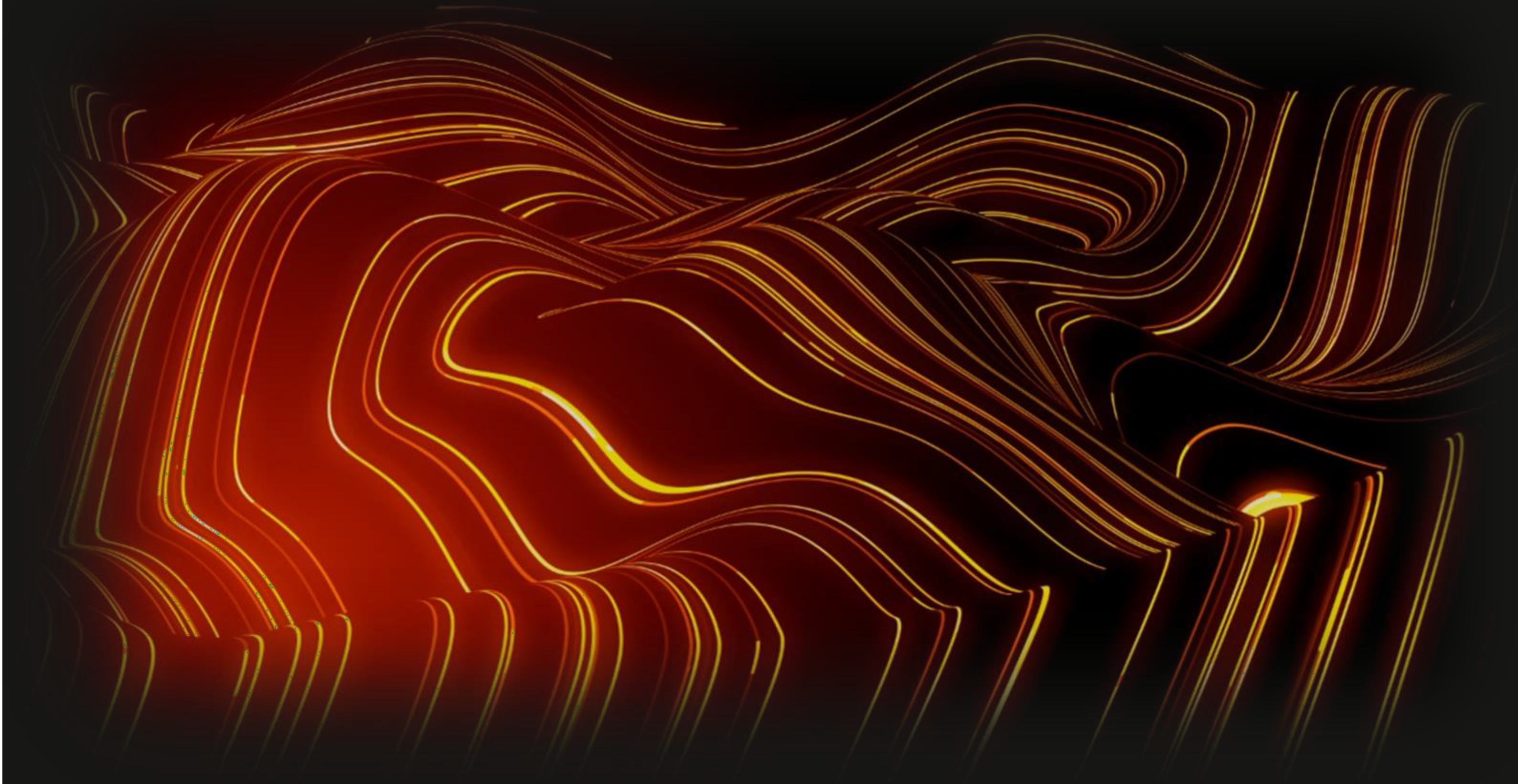
Ransomware in the Supply Chain: Six Lessons from 10 Years of Attacks

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

THOUGHT LEADERSHIP PAPER
SEPTEMBER 2025



Contents

Introduction

In 2015, Mastercard analysts cataloged two ransomware events. The first detonated in Houlton, Maine USA, targeting the town's Police Department. It shut down access to all documents and applications after the Houlton Police Chief opened a malicious email attachment. The ransom asked was $588 in Bitcoin.

Since then, Mastercard has cataloged and analyzed a total of 7,158 ransomware events, some with ransoms ranging into the tens of millions of US dollars. These include incidents that crippled delivery of energy and utility services, forced shutdowns of numerous K12 schools and universities, degraded capabilities at hospitals, and halted food production. Many of the events impacted entire supply chains, damaging organizations beyond the boundaries of their direct victims.

The details of these ransomware events contain valuable lessons for better managing enterprise cybersecurity risks for the own enterprise and the supply chain. Even if one's own cybersecurity house is in order, the reality of uneven cybersecurity strength in the supply chain leaves risk managers to answer critical questions, such as: How resilient is my supply chain to ransomware? Which of my hundreds of suppliers represent the greatest risk? What should I do to address the risks?

Managing risks well requires good information upon which managers can build models and protocols for efficiently guiding their organizations to good risk positions. To that end, the RiskRecon by Mastercard research team has distilled six important insights for managing supply chain risk from these 7,158 ransomware events. These same lessons apply equally to one's own enterprise cybersecurity risk posture.

1. The recent odds of a company succumbing to a damaging ransomware event in a 12-month period are about one percent.

2. Good cybersecurity hygiene pays well; organizations earning an A-rating by RiskRecon have a 5.3 times lower frequency of ransomware events.

3. No industry is safe. Criminals are targeting every industry – construction, energy, education, entertainment, healthcare, manufacturing.

4. No geography is safe. Criminals hit organizations in 134 different countries.

5. Ensure that your operationally important suppliers have 24x7 security operations; criminals are detonating ransomware seven days a week, and they aren't taking a break for the holidays.

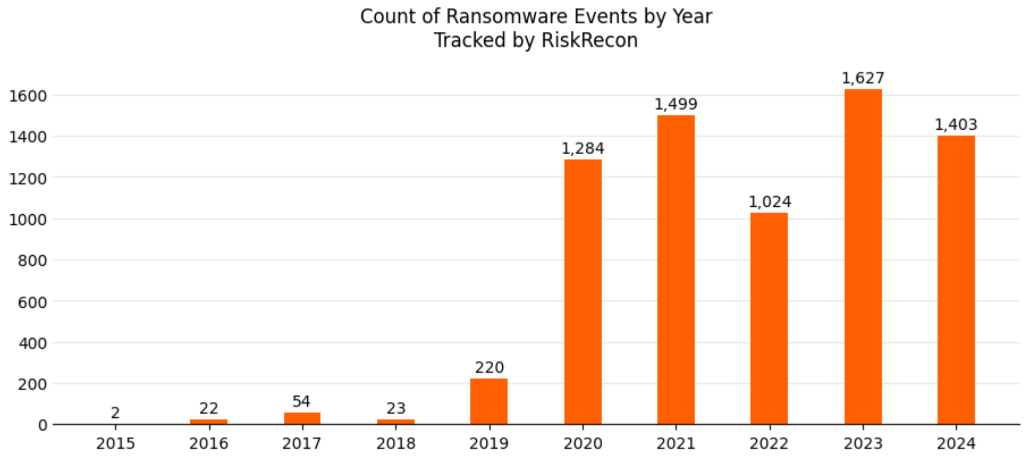
6. Settle in for the long haul; 2024 saw a record number of active ransomware gangs.

We all have a shared responsibility in managing the risk of ransomware because no enterprise exists in isolation. Perhaps one of the greatest services that a cybersecurity team can render after ensuring their own house is in order is to help their suppliers and partners protect theirs. As is always the case when serving, where you give you gain. That is central to the work of managing third-party risk.

The Study

RiskRecon continuously monitors the cybersecurity hygiene of over seven million organizations, spanning all industries and nearly all parts of the globe. For this study, we selected 196,000 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.

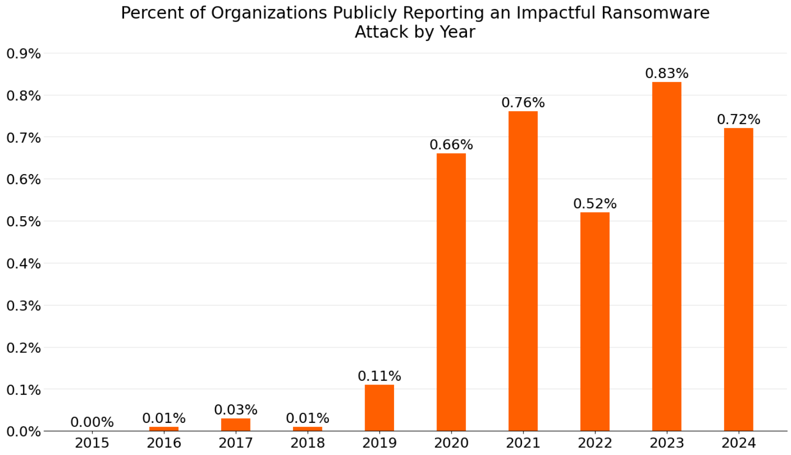
RiskRecon cataloged and studied 7,158 publicly reported ransomware events that occurred between January 2015 and December 2024. These events were identified through internet keyword searches, monitoring of event disclosure sites, dark web and open web ransomware sites, local and international news sites, and 8K SEC filings.



For purposes of this study, a ransomware event is 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.

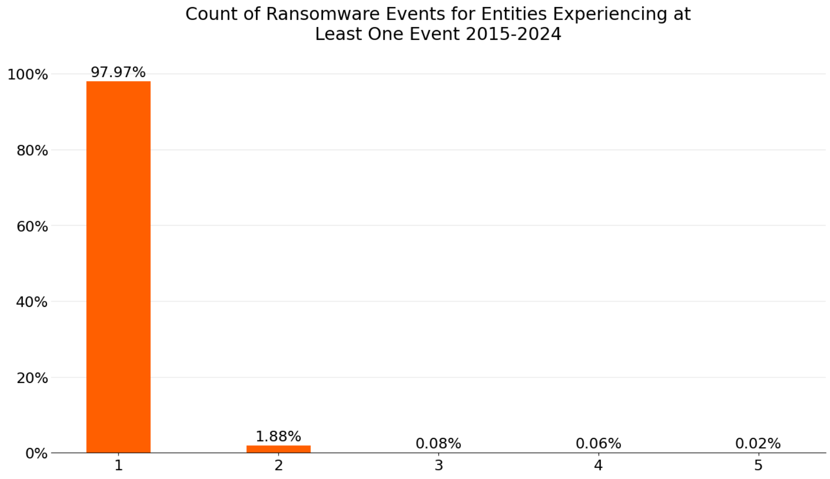
Lesson 1: About one in one hundred chances

Across the last ten years 3.6% of companies are publicly known to have fallen victim to an impactful ransomware attack. The annual rate has grown from near zero in 2015 (2 of 196,000 organizations) to a 10-year high in 2023 of 0.83% - 83 of every 1,000 organizations in the study. 2024 closed out at 0.72% companies falling victim to ransomware.



Considered within the context of a supply chain, expect that each year one of every 100 suppliers will succumb to an attack through which it loses control of their systems or data at the hands of a ransomware gang. Larger companies that have hundreds of suppliers could be dealing with five, ten, or more ransomware shocks to their supply chain each year.

The graph below shows the count of ransomware events for entities that had at least one event. Among the 3.6% of organizations that were hit with ransomware during the last 10 years, two percent of those organizations were hit more than once. So, the probability of an organization falling victim more than once in 10 years is 0.072% (3.6% x 2%). 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.



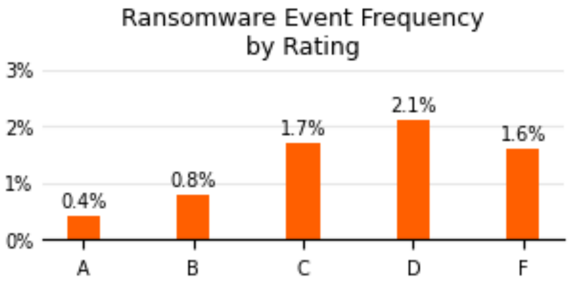
Lesson 2: Good cybersecurity hygiene pays well

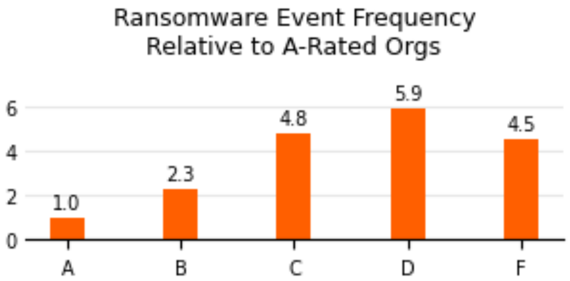
RiskRecon had visibility into the cybersecurity hygiene of 1,914 of ransomware attack victim organizations at the time of the incident. Based on this data, those with very poor cybersecurity hygiene, rated by RiskRecon as D or F, experienced a 5.3x higher frequency of ransomware events compared to A-rated organizations, which RiskRecon observes as having very clean hygiene. Just over 2% of D and 1.6% of F-rated companies have had a ransomware event from 2015 through 2024. In comparison, only 0.4% of A-rated companies and 0.8% of B-rated companies suffered a ransomware event.

Organizations with good cybersecurity hygiene have

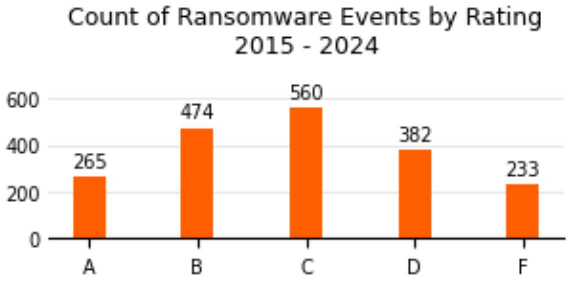
5.3X lower

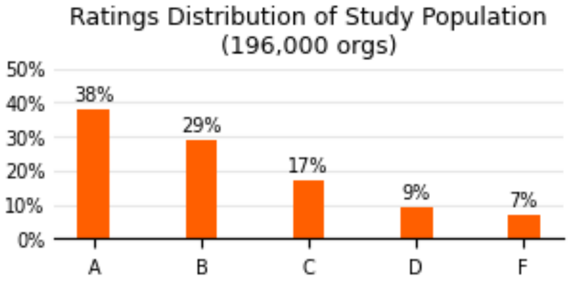
frequency of ransomware events





Lest one think that the larger populations of A and B rated organizations are skewing the correlation, across the population of 196,000 entities, A-rated organizations have a 5.4 times larger population than F-rated while having about the same number of ransomware events. The graphs of event counts by rating and the rating distribution of the 196,000 entities 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 system-encrypting ransomware attack. In comparison with the general population, those that succumb to ransomware, on average, have:

- 14.7 times more high and critical severity issues in their internet facing systems.
- 8.6 times more unsafe network services exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.
- 8.7 times higher frequency of encryption configuration issues in high value systems that collect and transmit sensitive data.
- 8.8 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.

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

	Average Issue Count		
	Ransomware Victim	General Population	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	11.8	0.8	14.7x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	19.8	2.3	8.6x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	20.3	2.3	8.8x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	37.4	4.3	8.7x higher

Ignoring issue counts and just looking at the percent of companies with one or more issue across the cybersecurity domains, the ransomware victim group again stands out as having very poor hygiene in comparison to the general population.

- 3.1 times more organizations with at least one high or critical severity software vulnerability in their internet facing systems.
- 2.4 times more organizations with at least one unsafe network service exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.
- 1.6 times more companies with at least one application security issue such as not implementing encryption in systems that collect sensitive data and application platform administration interfaces exposed to the internet with single-factor authentication.
- 2.2 times more companies with at least one web application that transmits sensitive data that has HTTP encryption issues such as expired certificates, weak encryption algorithms, or invalid certificate subjects.

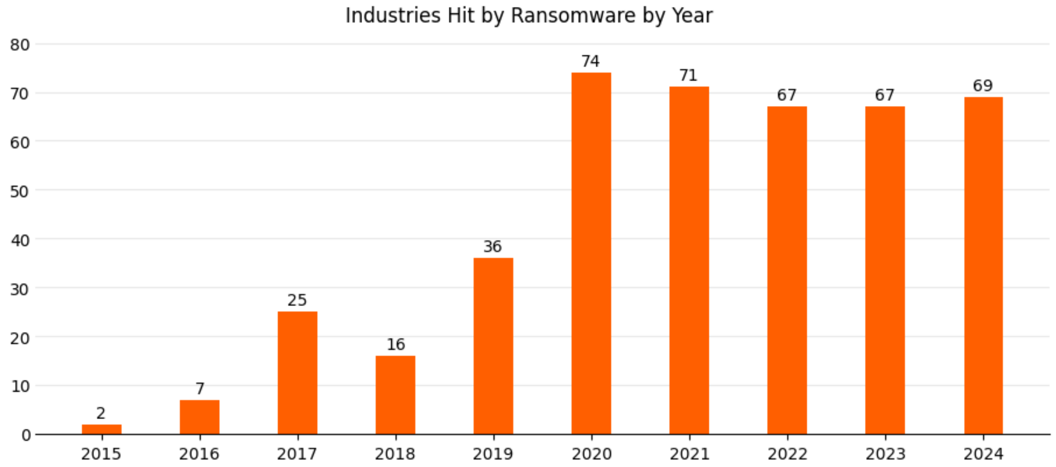
Table: Comparison of percent of organizations with at least one issue in their internet-facing systems

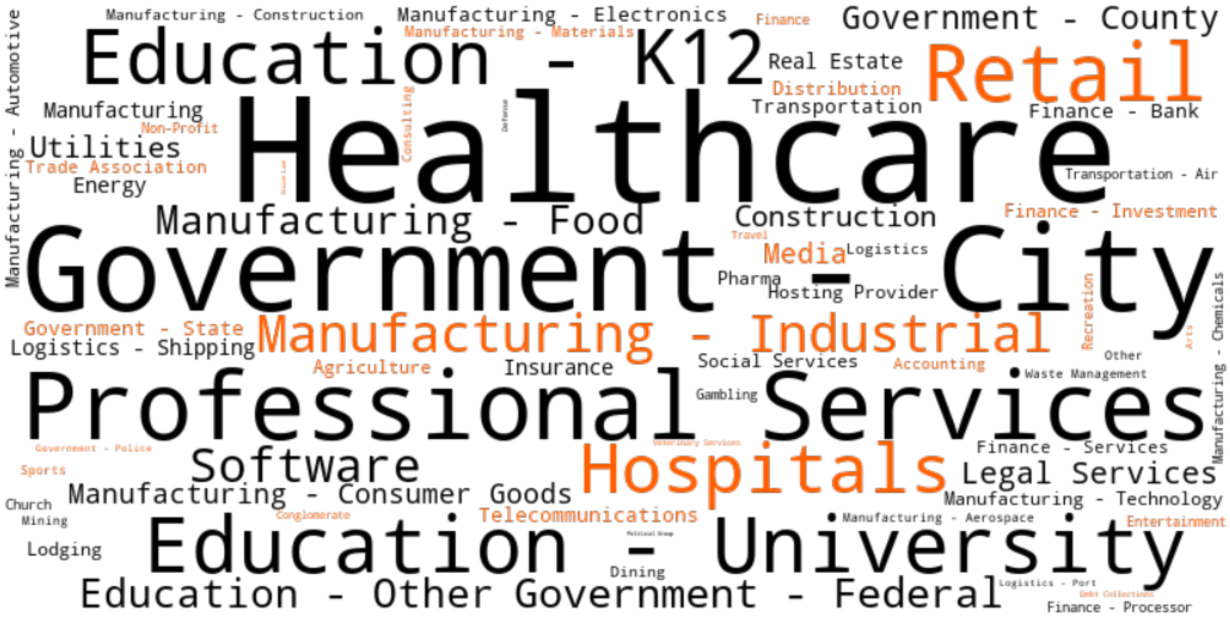
	Percent with at Least One Issue		
	Ransomware Victim	**General Population**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	47%	15%	3.1x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	45%	19%	2.4x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	55%	34%	1.6x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	62%	28%	2.2x higher

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 that are intent on crippling their operations and steal sensitive data. 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.

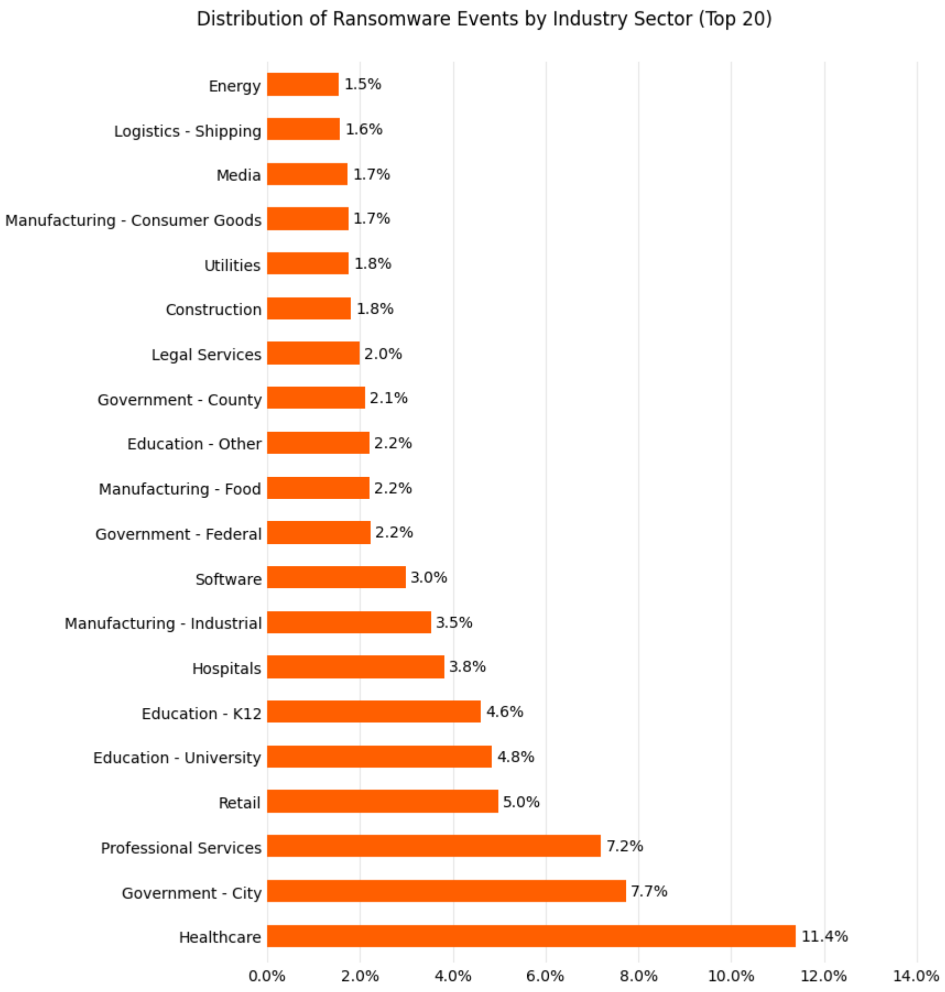
Lesson 3: Criminals are targeting every sector

Across the 7,158 ransomware events occurring from 2015 to 2024, criminals disrupted the operations of organizations across 81 different industry sectors. In 2015, just two industries were hit: utilities and police. As of 2024, the victim list has expanded to include casinos, hotels, local fire and police departments, agriculture, and cruise lines. Even veterinary clinics succumbed to ransomware.





Unfortunately for society, healthcare providers have been the most frequent victim, accounting for more than 11% 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 11.6% of events. City governments have also taken a heavy hit, accounting for 7.7% of all ransomware events.

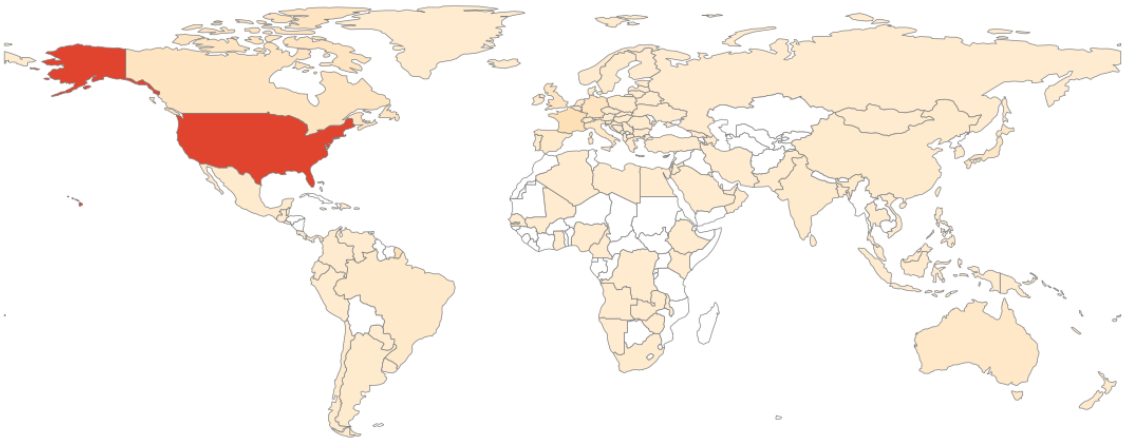

Distribution of Ransomware Events by Industry Sector (Top 20)

Regardless of the industry one operates in, every company is a candidate for destruction at the hands of cybercrime groups. Know and protect your operationally sensitive systems, even beyond those that store and process sensitive data and transactions. The criminals will target them.

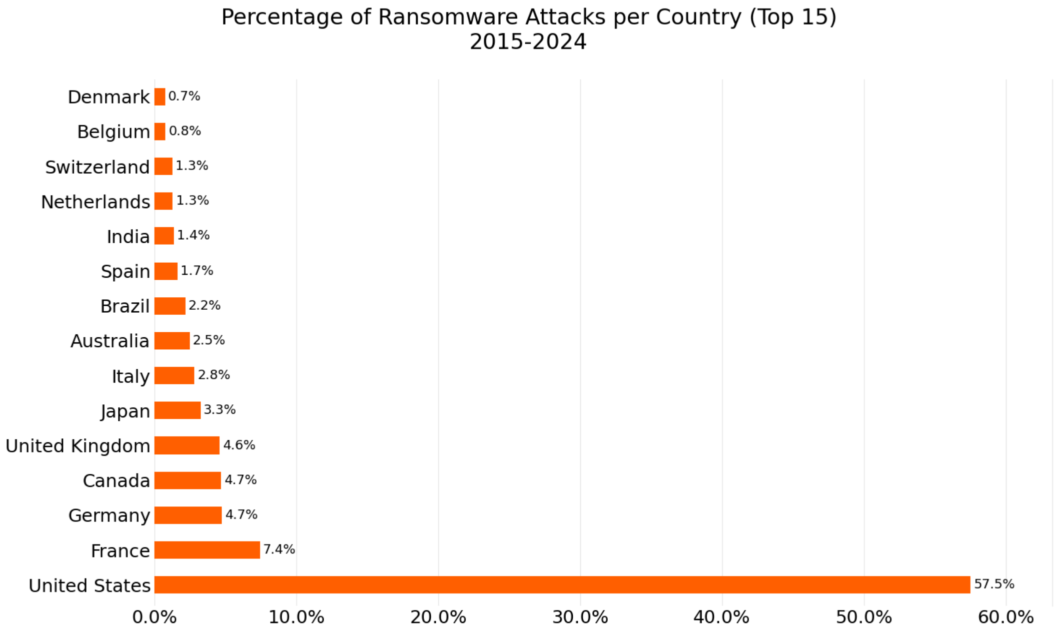
And the same holds true for the supply chain. Each vendor and partner are a possible target. Know the ones you are operationally dependent on. Those suppliers that were previously rated as low inherent risk due to lack of data or transaction sensitivity might be high or critical when examined through the lens of operational dependency.

Lesson 4: Criminals are hitting every geography

Criminals are striking organizations in nearly every geography. RiskRecon cataloged ransomware events in 134 countries. While the bulk of the attacks follow the level of economic activity, some did reach 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.

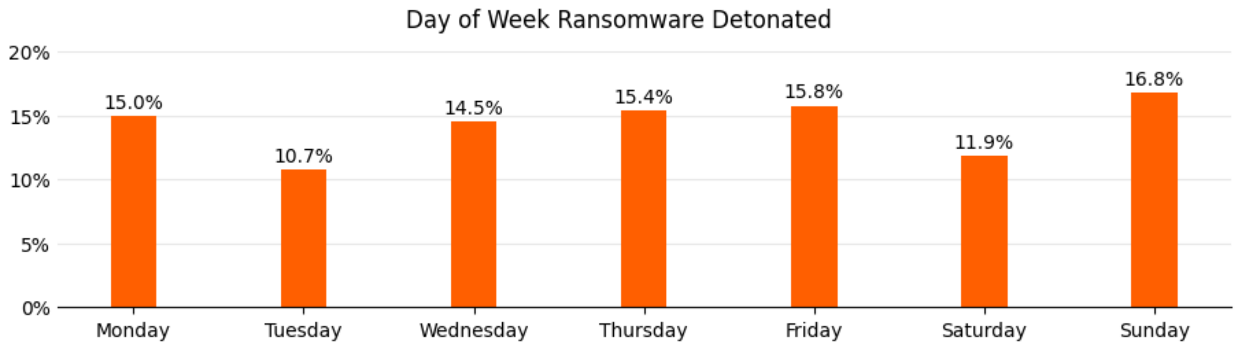


Most publicly reported ransomware attacks hit US-based organizations, accounting for 57.5% of the total. France came in next at 7.4% followed by Germany and Canada at 4.7% and the UK at 4.6%.

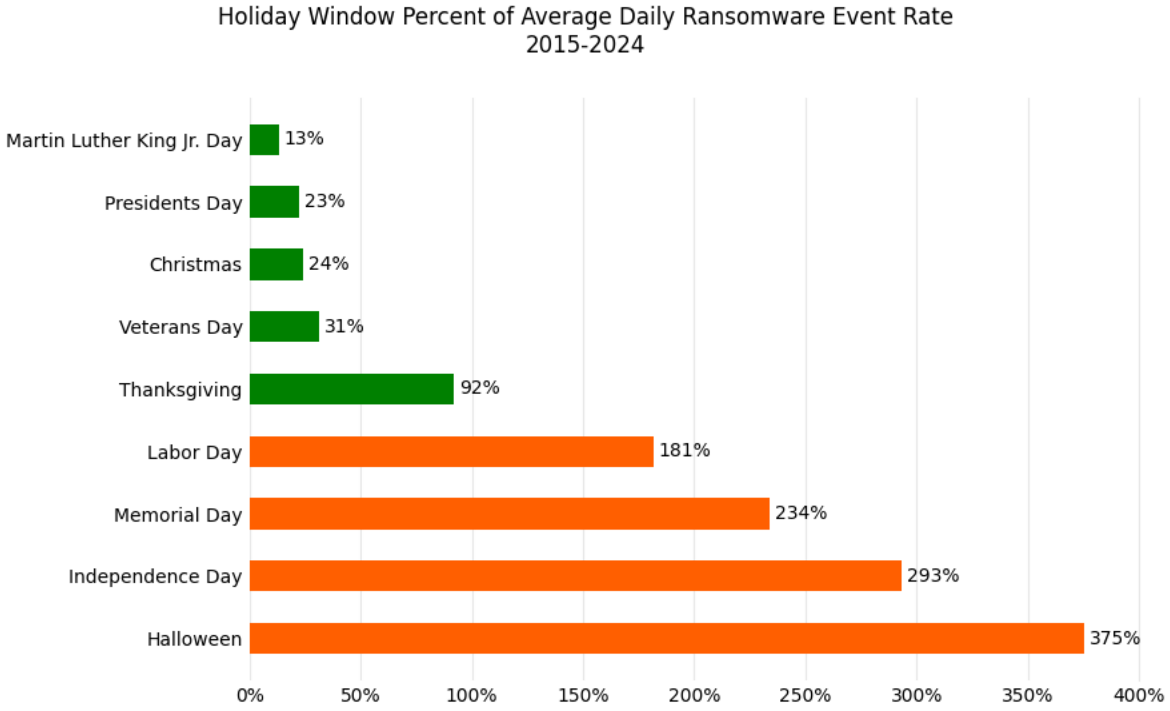


Lesson 5: 24x7 security operations is essential

Criminals are detonating ransomware seven days a week, with no day of the week having less than 10% of the total events. Sundays came in the highest at 16.8% of all events, nearly 20% higher than its fair share of an evenly divided week.



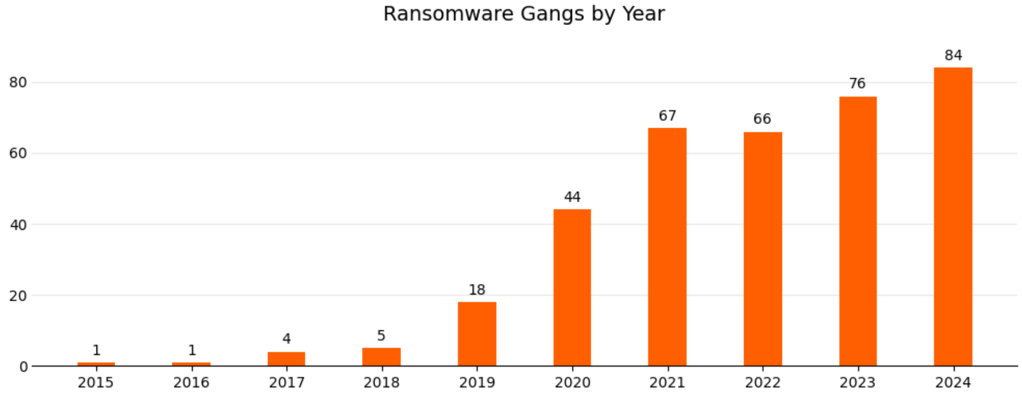
Criminals aren't taking the holidays off either. Looking at the week surrounding the major U.S. holidays, with the holiday date at the center of the week, four of the nine holidays analyzed have a higher daily breach event rate than an average day. Memorial Day, Independence Day, and Halloween all more than double the daily average breach rate.

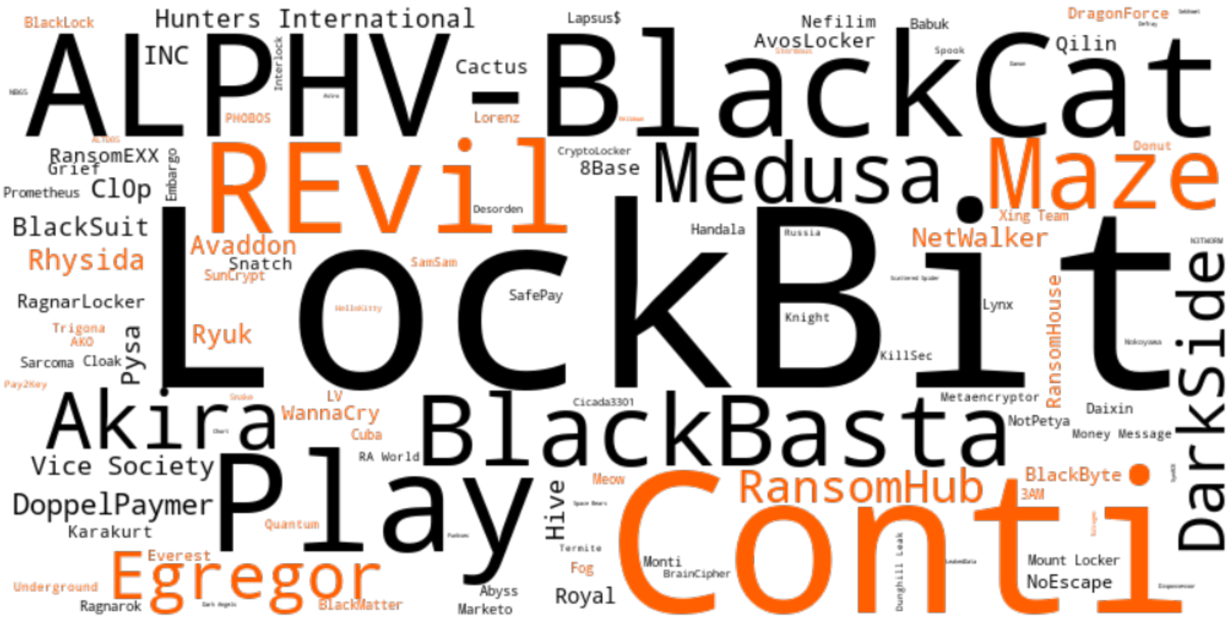


Ensure that your operationally important suppliers have 24x7 IT and security operations every day of the year, including holidays. Rapid response to a ransomware event is essential to limiting damage and getting on with recovering systems and operations.

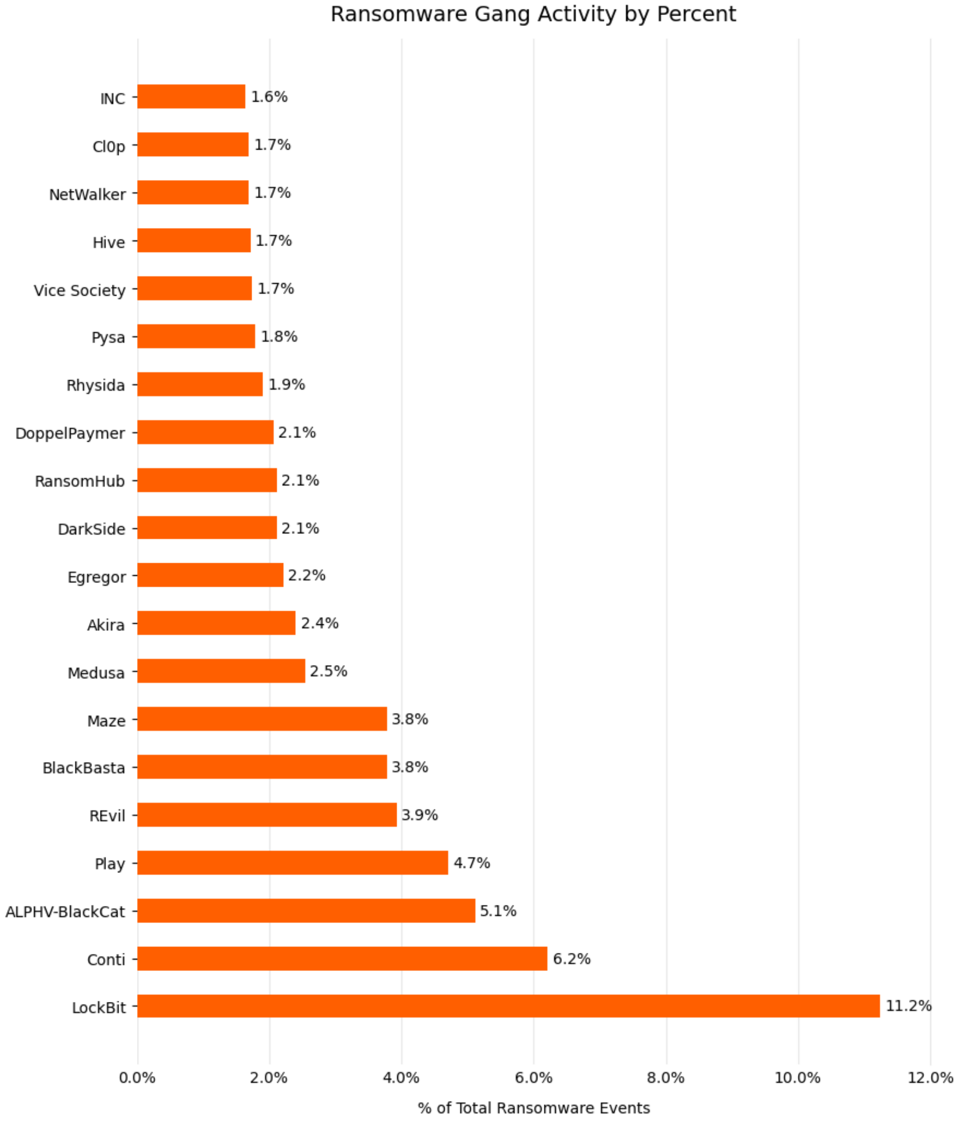
Lesson 6: Settle in for the long-haul

The number of resources criminals are directing towards ransomware attacks is growing dramatically. From 2015 through 2024 there were 214 different criminal groups behind the 7,158 publicly reported ransomware events cataloged by RiskRecon. In 2017 there were only four. There were 86 active groups identified in 2024.


Ransomware Gangs by Year



Lockbit has been the most active group, accounting 11.2% of all cataloged events in which the threat actor was disclosed, 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 coming on the scene in 2019 and remaining active through 2024.



So, what does it mean to settle in for the long haul in the battle against ransomware? Update the foundations of your program to account for the threat of ransomware. Those foundations are your risk models, your information security standards, your policies and procedures, and your security assessment criteria and related questionnaires. Most of the capabilities for managing ransomware in the supply chain are likely already in your own program, as they are the basics of managing IT and cybersecurity well. It is just that it is now more important than ever to ensure your suppliers are doing the basics well.

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).

Conclusion

No company can operate well without its suppliers reliably delivering their goods and services. Ransomware threatens the operations of nearly every vendor in the supply chain. Fortunately, successfully managing the risk of ransomware requires doing the basics of IT and cybersecurity well. Unfortunately, so many organizations do not.

The threat of ransomware significantly increases the importance of managing supply chain cybersecurity risk well. The primary challenge of managing supply chain cybersecurity risk well is scale. Supply chains span tens, hundreds, and sometimes thousands of organizations.

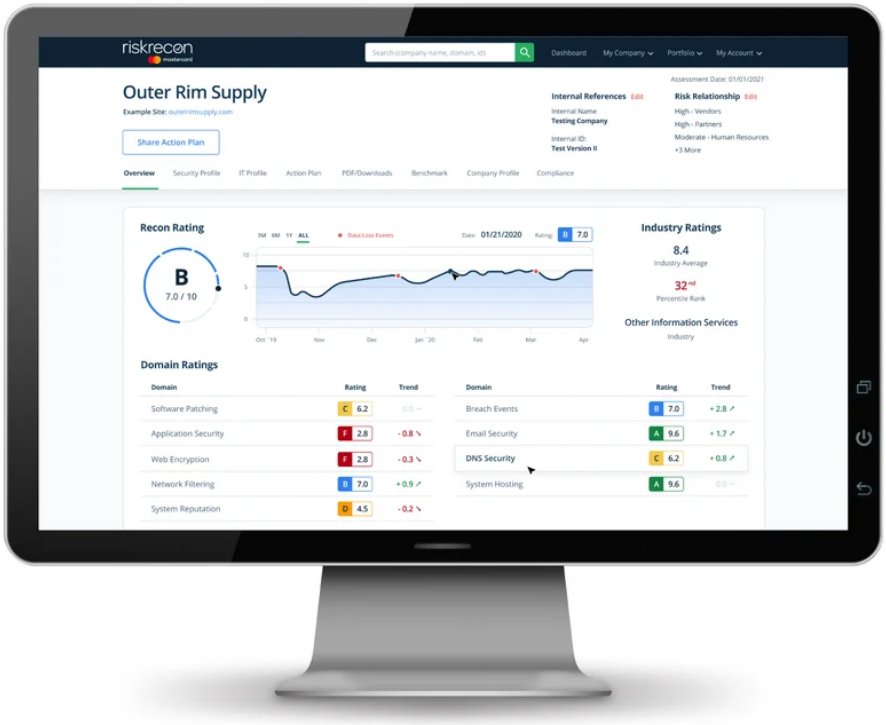
Leverage the intelligence and predictive insights of the RiskRecon cybersecurity ratings and assessment platform to identify the suppliers with poor cybersecurity hygiene; these are the ones that are going to have dramatically higher rates of ransomware and data loss events.

Factoring in the criticality of your suppliers, prioritize assessment of the poor performers and determine if they are going to improve or if you should find other partners. RiskRecon's detailed assessments will help you in your engagements by pinpointing the hot spots.

Remember, you can outsource your systems and services, but you cannot outsource your risk. RiskRecon helps you achieve better supply chain risk outcomes at scale.

About RiskRecon by Mastercard

RiskRecon by Mastercard enables you to easily achieve better risk outcomes for your enterprise and your supply chain. RiskRecon's cybersecurity ratings and assessments make it easy for you to understand and act on your risks, delivering accurate, risk-prioritized action plans custom tuned to match your risk priorities. Learn more about RiskRecon and request a demo at www.riskrecon.com.



Outer Rim Supply

Example Site: outerrimsupply.com

Assessment Date: 01/01/2021

Internal References Edit

Internal Name
Testing Company

Internal ID:
Test Version II

Risk Relationship Edit

High - Vendors
High - Partners
Moderate - Human Resources
+3 More

Recon Rating

B
7.0 / 10

Date: 01/21/2020 Rating: B 7.0

Industry Ratings

8.4
Industry Average

32nd
Percentile Rank

Other Information Services
Industry

Domain Ratings

Domain	Rating	Trend
Software Patching	C 6.2	0.0 →
Application Security	F 2.8	- 0.8 ↘
Web Encryption	F 2.8	- 0.3 ↘
Network Filtering	B 7.0	+ 0.9 ↗
System Reputation	D 4.5	- 0.2 ↘

Domain	Rating	Trend
Breach Events	B 7.0	+ 2.8 ↗
Email Security	A 9.6	+ 1.7 ↗
DNS Security	C 6.2	+ 0.8 ↗
System Hosting	A 9.6	0.0 →

This document is proprietary to Mastercard and shall not be disclosed or passed on to any person or be reproduced, copied, distributed, referenced, disclosed, or published in whole or in part without the prior written consent of Mastercard. Any estimates, projections, and information contained herein have been obtained from public sources or are based upon estimates and projections and involve numerous and significant subjective determinations, and there is no assurance that such estimates and projections will be realized. No representation or warranty, express or implied, is made as to the accuracy and completeness of such information, and nothing contained herein is or shall be relied upon as a representation, whether as to the past, the present, or the future.