riskrecon

mastercard

RiskRecon Rating Correlation to Destructive Ransomware Event Frequency

Managing the risk of destructive ransomware in the supply chain with RiskRecon cybersecurity ratings and insights

Q4 2022

riskrecon.com

sales@riskrecon.com

Introduction

Criminals are targeting organizations of all shapes, sizes, industries, and geographies with system-encrypting ransomware attacks, holding their ability to operate to ransom. It is common to hear of ransomware attacks rendering hospitals unable to provide care, governments unable to legislate, manufacturers unable to produce products, SaaS applications unable to operate, and schools unable to educate. You don't have to have your systems encrypted in a ransomware attack to have your operations impacted. A destructive ransomware attack against one of your critical suppliers could harm your ability to operate.

The reality of uneven cybersecurity strength among vendors and limited visibility into the details of each vendor leaves risk managers to answer critical questions for the enterprise. 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? Perhaps the most challenging dimension of all is that supply chain risk must be managed with limited resources and with limited visibility into suppliers' operations.

To help understand the probability of an organization succumbing to a destructive ransomware attack, RiskRecon has conducted several studies of the cybersecurity hygiene of companies at the time of the detonation of the ransomware in their organization using the RiskRecon cybersecurity ratings platform. To date, RiskRecon has studied a total of 993 public-reported destructive ransomware events occurring between January 2016 and October 2022. Of these 993 events, RiskRecon had visibility into the cybersecurity hygiene of 606 organizations at the time of ransomware detonation.

By comparing the cybersecurity hygiene of victims with that of RiskRecon's larger population of about 180,000 organizations, RiskRecon determined if the Internet-observable cybersecurity hygiene of an organization is a material factor in their expected frequency of succumbing to a destructive ransomware attack.

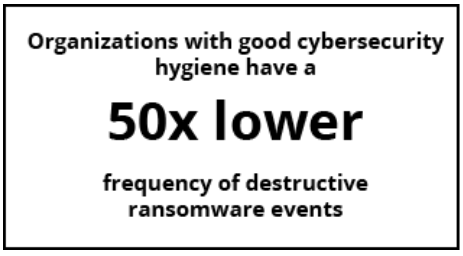
In case you don't want to read the whole study, here is main event:

Question: How do you minimize the likelihood of your key vendors falling victim to a destructive ransomware attack?

Answer: Do business with vendors that practice good cybersecurity hygiene. As measured by RiskRecon, companies with good cybersecurity hygiene have a 50 times lower rate of destructive ransomware events in comparison with companies that have very poor hygiene.

Question: But, how do you know which vendors don't have good cybersecurity hygiene?

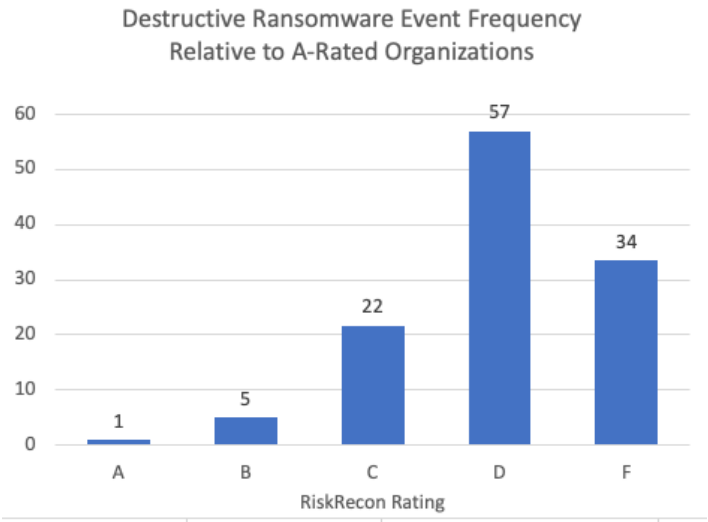
Answer: Use RiskRecon. It continuously assesses and measures the cybersecurity hygiene of any organization with internet-facing systems. RiskRecon's rating model strongly predicts the relative frequency of destructive ransomware events to expect for each of your vendors.



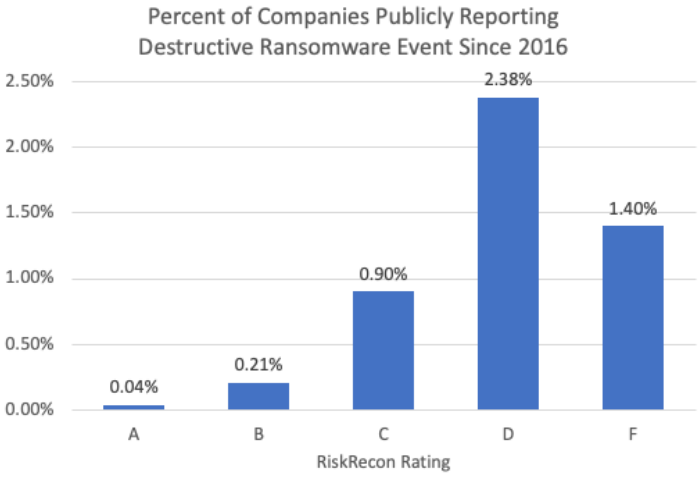
The following sections detail the study findings, including rating correlation and cybersecurity conditions of ransomware victims, and the study methodology. We also talk about why it is that companies with poor hygiene are succumbing to destructive ransomware attacks so much more frequently.

Ratings Correlation

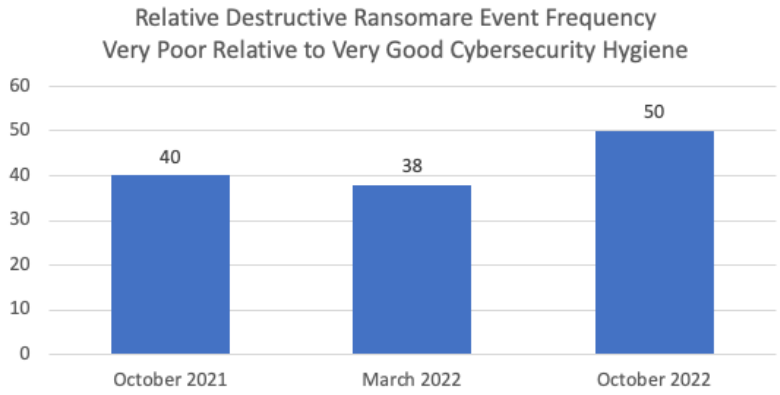
RiskRecon provides a powerful capability for better managing ransomware risks in the supply chain. RiskRecon's rating model strongly predicts the destructive ransomware event frequency within a vendor population. Based on an analysis of the RiskRecon ratings and ransomware events occurring across 179,914 organizations, companies in the "F" and "D" rating tiers have a 50 times higher rate of ransomware events than do "A" rated companies.



Organizations with clean cybersecurity hygiene, earning a RiskRecon rating of "A", had a destructive ransomware event frequency of 0.04% (0.4 for every 1,000 organizations). Those with very poor cybersecurity hygiene, those with a RiskRecon rating of "D" or "F", had a system-encrypting ransomware event frequency of 2.1%. Said differently, a whopping 21 of every 1,000 D or F-rated companies had a destructive ransomware event in the last seven years. Again, that is 50x higher than A-rated companies and 8.5x higher than the general population!



The correlation between RiskRecon ratings and ransomware event frequency continues to strengthen over time. In RiskRecon's study conducted in October 2021, covering 389 events, companies with very poor cybersecurity hygiene ("D" or "F" rated) had a 40 times higher frequency of destructive ransomware events compared with companies with very good hygiene ("A" rated). In the study conducted in March 2022, spanning 470 events, the relative frequency decreased slightly to 38 times higher. In this latest study covering 606 events, the frequency of destructive ransomware events for organizations with very poor hygiene grew to 50 times higher in comparison with companies with good hygiene.



Underlying Cybersecurity Conditions

Cybersecurity ratings are an abstract representation of the quality of an organization's security hygiene, but what does a cybersecurity rating of D or F look like? To make it concrete, let's look at the underlying cybersecurity conditions of victims of ransomware on the day of detonation and compare it with the general population of 179,914 companies. Victims of destructive ransomware, on average, have:

11 times more high and critical severity software vulnerabilities in their internet-facing systems.

5.3 times more unsafe network services exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.

9 times higher rate of malicious activity such as botnet communications emanating from their systems to the internet.

9.2 times higher count of web applications that collect sensitive data that have material encryption issues such as expired certificates, weak encryption algorithms, and invalid certificate subjects.

The table below compares the cybersecurity hygiene of internet-facing systems of ransomware victims at the time of detonation with the general population across seven security domains. The metric "percent with issues" is the percent of companies with at least one occurrence of the issue in their internet-facing systems. The metric "average issue count" is the average number of issues observed in their internet-facing systems.

Table: Average Cybersecurity Conditions in Internet-facing Systems
Destructive Ransomware Victims Compared with General Population

	Ransomware Victim		General Population	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	percent with issues	57%	18%	**3.2x higher**
	average issue count	21.3	1.9	**11x higher**
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	percent with issues	53%	29%	**1.8x higher**
	average issue count	23	4.3	**5.3x higher**
Application Security Issues Missing common security practices in applications that collect sensitive data	percent with issues	45%	37%	**1.2x higher**
	average issue count	16.6	2.1	**7.9x higher**
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	percent with issues	75%	39%	**1.9x higher**
	average issue count	35.0	3.8	**9.2x higher**
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	percent with issues	65%	36%	**1.8x higher**
	average issue count	7.6	1.3	**5.8x higher**
DNS Security Issues Active domains (domains that are not parked) missing domain hijacking protection	percent with issues	42%	20%	**2.1x higher**
	average issue count	2.7	0.6	**4.5x higher**
System Reputation Issues Number of systems exhibiting malicious activity such as communicating with botnet controllers, block-listed for attempting to compromise other systems or spamming.	percent with issues	11%	2%	**5.5x higher**
	average issue count	9.0	1.0	**9x higher**

Why Such a Strong Correlation?

Companies with very poor hygiene have a 50 times higher frequency of destructive ransomware events relative to companies with good hygiene! Why is there such a strong correlation between cybersecurity hygiene and ransomware event frequency?

Detonating system encrypting ransomware within the systems that will materially harm the operations is not trivial if security shields are up. First, the criminals must gain an initial foothold in the environment. From that initial foothold, the criminals must pivot around the network to identify and compromise a system or systems that will impact operations. No doubt, companies with good hygiene fall victim, but they have a much lower rate of impactful destructive ransomware events because their environments are harder to compromise, and they are more likely to have detective controls that detect the compromise before it escalates to ransomware detonation.

CoveWare, a leading ransomware incident response firm, confirms in its Q2 2022 research paper that criminals are exploiting common cybersecurity hygiene issues to gain their foothold in an organization. Their data on the initial compromise vector attributes 35% to email phishing, 30% to RDP compromise, 20% to software vulnerability exploitation, and 15% to other. Read the CoveWare research at https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

The US Cybersecurity and Infrastructure Security Agency reemphasized doing the basics well in their 2021 ransomware advisory (https://www.cisa.gov/uscert/ncas/alerts/aa22-040a). Keep software up to

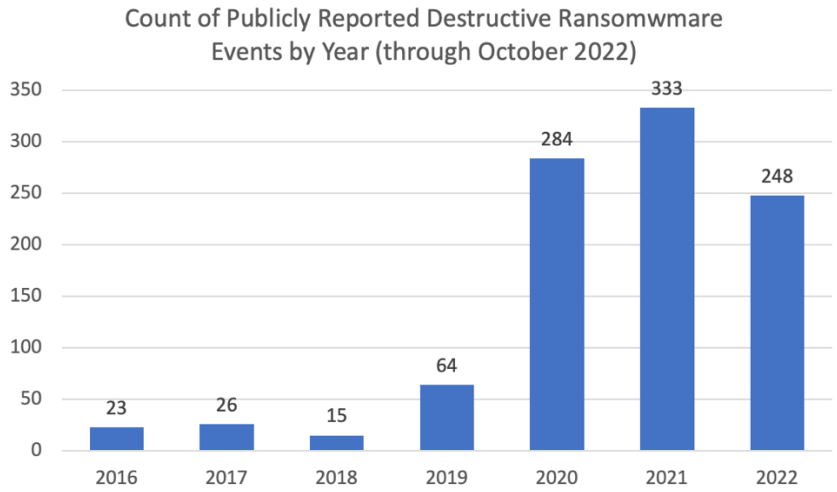
date, don't expose RDP to the Internet, require multi-factor authentication for remote access, and operate an email phishing defense program.

Study Methodology

RiskRecon continuously assesses the cybersecurity hygiene of enterprises, rating their performance on an A – F scale across domains such as vulnerability management, network filtering, application security, and web encryption. RiskRecon did not set out to build a model to predict ransomware events. Rather, the rating model is designed to measure the quality of the organization's cybersecurity risk management as observed in the reality of "known good" and "known poor" risk management performance. For example, banks are known to manage risk better than universities. You can read about RiskRecon's rating model here

https://www.riskrecon.com/cybersecurity-risk-rating-model.

RiskRecon researchers identified 993 publicly reported destructive ransomware events that resulted in the encryption of the victim organization's systems, occurring between January 2016 and October 2022. These publicly reported events were identified through internet keyword searches, monitoring of event disclosure sites, dark web sites, and 8K SEC filings. Events in which the impact was limited to data theft were excluded.



Of the 993 destructive ransomware events, RiskRecon observed the cybersecurity hygiene and rating for 606 of the victims at the time of ransomware detonation. This data was then compared against the total population of 179,914 companies and their ratings at the end of the study window.

Conclusion

Maintain good cybersecurity hygiene within your organization. Do business with vendors who have good cybersecurity hygiene. The data clearly shows that doing so will dramatically reduce the frequency with that your organization is impacted by destructive ransomware within your organization and your supply chain. Organizations with good cybersecurity hygiene have 50 times lower frequency of ransomware events compared with organizations that poor hygiene.

RiskRecon's continuous cybersecurity ratings and assessments make it easy to understand and act on your risks, enabling you to easily achieve better risk outcomes. Instantly shine a light on your supply chain and find out which ones are managing your risks well and which ones are exposing you to unacceptable risks. Share the assessment with your vendors to help them improve their program and automatically monitor their progress.

About RiskRecon, a Mastercard Company

RiskRecon, a Mastercard Company, enables you to achieve better risk outcomes for your enterprise and your digital 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.