riskrecon

mastercard

Managing the Risk of Ransomware in the Supply Chain

Five lessons from analysis of 633 publicly disclosed destructive ransomware events

riskrecon.com

sales@riskrecon.com

Introduction

The impact of a destructive ransomware attack extends far beyond the organization whose systems are encrypted. It harms all those who depend on the goods and services of the organization that criminals have taken offline.

Much has been written about hardening enterprises against the threat of ransomware, but what about protecting supply chains? Ideally, every supplier has a robust security program, strong ransomware defense, and stout resilience measures in place. Unfortunately, as we have learned in the face of other threats, this is not the case.

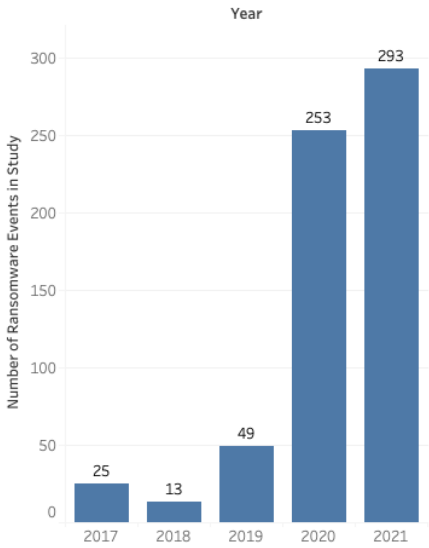
The reality of uneven cyber security strength in the supply chain leaves risk managers to answer critical questions for the enterprise. How susceptible is my supply chain to ransomware? Which of my hundreds of suppliers represent the greatest risk? What should I do to address the risks? Perhaps the most challenging dimension of all is that risk managers must manage supply chain risk with limited resources and the disadvantage of assessing suppliers from the outside.

Solving risk at scale requires good information upon which risk managers can build models and protocols for efficiently guiding their organizations to good risk positions. To that end, our research team has distilled five important insights for better managing supply chain ransomware risk based on an analysis of 633 publicly disclosed ransomware events occurring between 2017 and 2021.

1) Do business with suppliers who have good cyber security hygiene; they have dramatically lower rates of destructive ransomware and data loss events.
2) Revisit your supplier inherent risk ratings to include operational dependency; criminals are targeting every sector.
3) Ensure that your suppliers have 24x7 ransomware protection, detection, and recovery operations; criminals are detonating ransomware seven days a week.
4) Don’t assume recent victims of ransomware materially improve their cybersecurity program; the data shows they make only marginal improvement in their cybersecurity hygiene one year after an event.
5) At the risk of stating the obvious, settle in for the long haul, the threat of ransomware is here to stay.

The Study

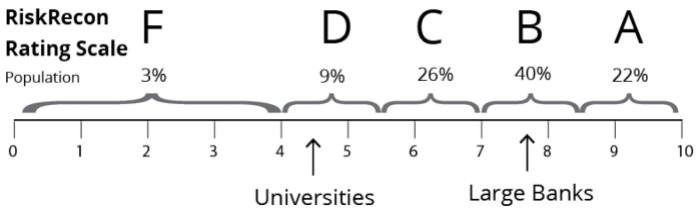
RiskRecon studied 633 publicly reported destructive ransomware events that occurred during the years 2017 through 2021. We did our best to include every publicly reported ransomware event for the years 2020 and 2021. The graph to the right shows the count of ransomware events distributed by year.



The benefit of limiting the study to publicly reported ransomware events, though excluding an untold number of unreported events, is that it inherently creates a population of events significant enough to be 'newsworthy'. We further limited the ransomware events studied to only those that impacted operations due to encryption of systems. Events that only resulted in a data breach, though important, were not included. In this study, we are particularly keen on understanding events that result in material disruption to operations – a new dynamic that managers of supply chain risk have to solve.

For each ransomware event, RiskRecon documented essential facts, such as the exact date of detonation, the criminal gang responsible, the ransom paid, the victim's industry and geography, and so forth. For each of the victim organizations, RiskRecon leveraged its continuous cybersecurity assessment and rating system to memorialize the cybersecurity hygiene at the time of the ransomware event. RiskRecon also analyzed the evolution of each organization's cybersecurity hygiene in the months and years following the attack.

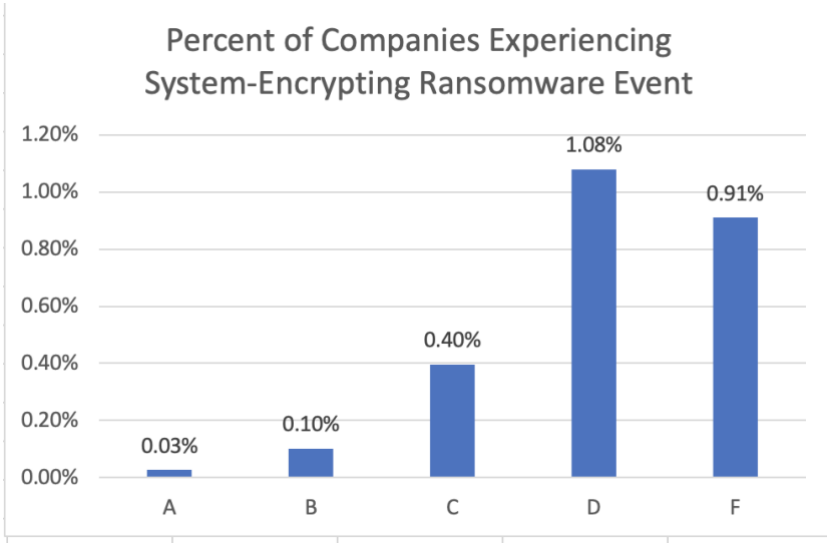
RiskRecon's assessments are based on a passive assessment of nine security domains and 40 security criteria spanning thousands of security checks. RiskRecon's assessment cover areas such as software patching, application security, web encryption, network filtering, and so forth. RiskRecon distills each assessment, detailing the IT profile, the security issues, and related severities, into a simple cybersecurity rating of A – F, with A being the best. The RiskRecon rating scale and the distribution of the total population of 100,000+ companies on which the model was built is shown below.



Insight 1: Do business with suppliers who have good cybersecurity hygiene

I once heard an advertisement for a car wash in which the company claimed that cars that are washed weekly last something like 30% longer than cars that are not cleaned regularly. On the surface, this seemed ridiculous, as there is no material link between the cleanliness of a vehicle and its useful life. I soon had the elementary ah-ha moment that people who wash their car frequently are much more likely to do regular maintenance. A clean car doesn't cause a car to last longer, but there is a positive correlation between owners who keep their car clean and owners doing regular maintenance which increases longevity.

And so it is with ransomware events. Based on RiskRecon's comparison population of cybersecurity ratings and assessments of over 100,000 entities, companies that RiskRecon observes to have very poor cybersecurity hygiene in their Internet-facing systems (a 'D' or 'F' RiskRecon rating) have about a 40 times higher rate of destructive ransomware events in comparison with companies that have clean cybersecurity hygiene. As shown in the chart below, only 0.03% of 'A-rated' companies were victims of a destructive ransomware attack, compared with 1.08% of 'D-rated' and 0.91% of 'F-rated' companies.



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 of 100,000 companies, the internet-facing systems of ransomware victims have an 11 times higher rate of material software vulnerabilities, 3.3 times higher rate of unsafe network services, and an 8.5 times higher rate of email security issues.

Table: Cybersecurity Conditions in Internet-facing Systems

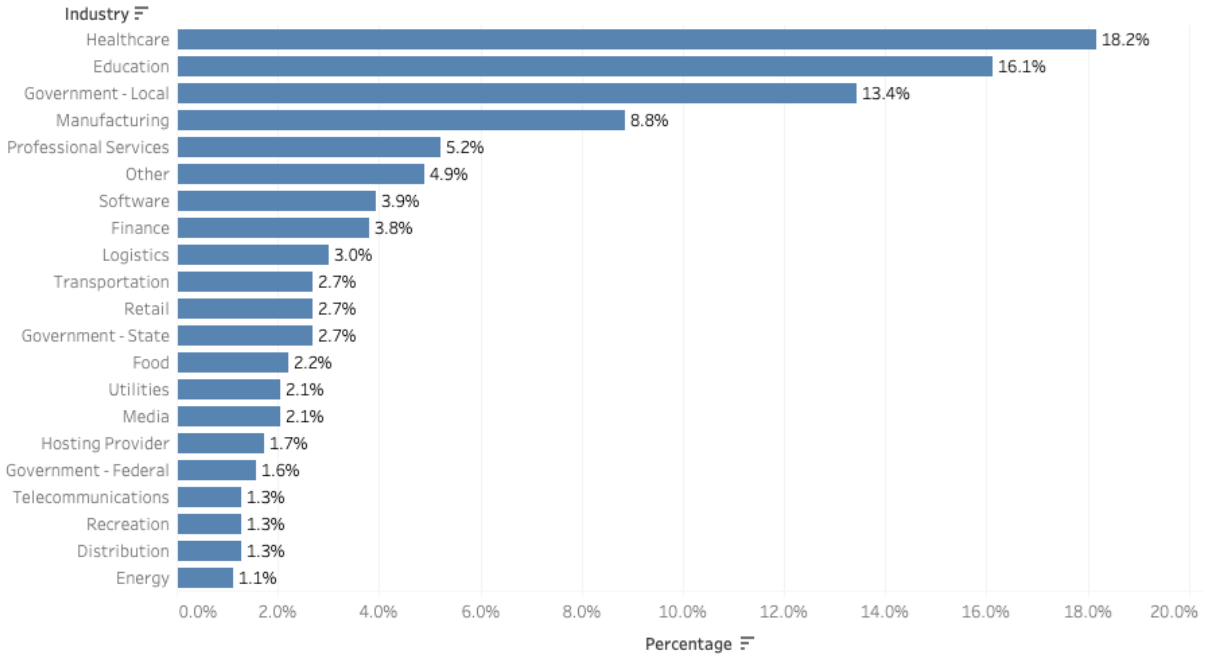
	Ransomware Victim		General Population	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of Medium or higher (7.0 – 10)	percent with critical issues	58%	19%	3.2x higher
	average issue count	11	1	11x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	percent with critical issues	33%	30%	0.1x higher
	average issue count	5	1.5	3.3x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	percent with critical issues	55%	36%	1.5x higher
	average issue count	9	2.3	3.9x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	percent with critical issues	74%	40%	1.9x higher
	average issue count	46	6.4	7.2x higher
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	percent with critical issues	68%	28%	2.4x higher
	average issue count	11	1.3	8.5x higher

While one or more of the issues outlined in the table above may not have been the vector by which criminals compromised the victim environment, the prominence of these issues is a strong indicator that the victim organizations are not operating robust cybersecurity risk programs. Just like dirty cars strongly correlate with poor maintenance, poor cybersecurity hygiene in Internet-facing systems strongly correlates with cybersecurity conditions that make the organization more susceptible to a successful ransomware attack.

Insight 2: Revisit your supplier inherent risk ratings; criminals are targeting everyone

I suspect that in the pre-ransomware world, most supplier inherent risk rating models were weighted primarily towards dimensions such as data types, transaction types, and related volumes. This model led organizations to focus their vendor risk management efforts on processors of sensitive data, relegating many operationally important suppliers to lower rating tiers. Ransomware has changed all that. From 2017 through 2021, according to an analysis of public reports, criminals successfully detonated ransomware in companies across 54 different industries.

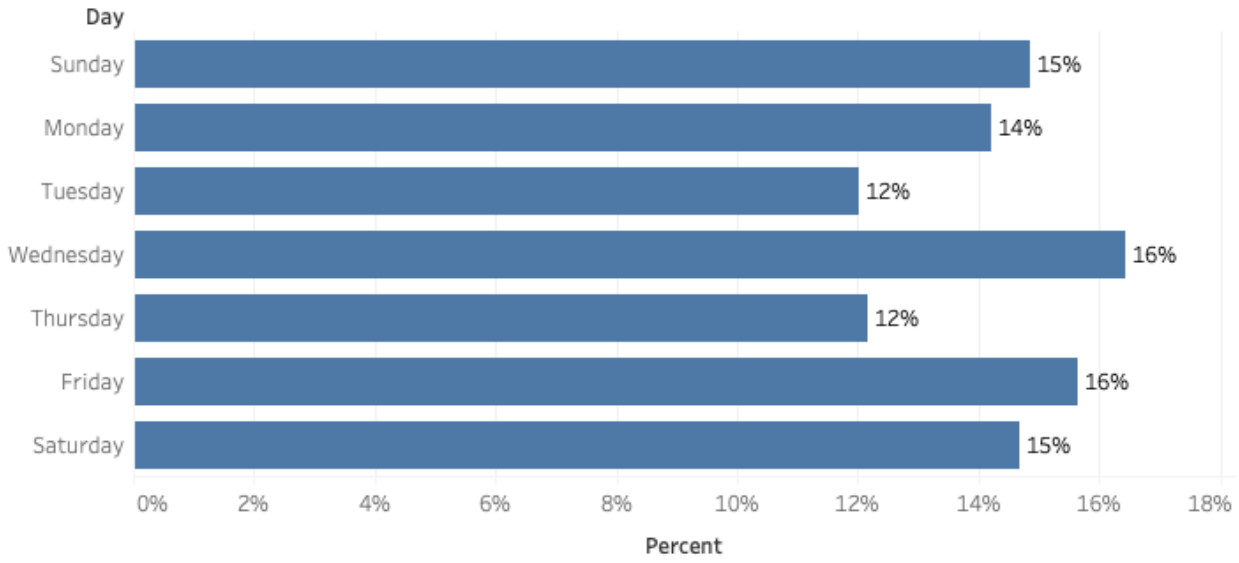
For sure, some industries are targeted more than others, with the healthcare and education sectors bearing the bulk of the successful attacks. Don't take too much comfort in that though, this analysis is based only on publicly reported events. The criminals are changing their tactics and their targets fast.



If you haven't done so already, do it now. Update your supplier inherent risk rating model to factor in operational dependency and apply the new model to every vendor. Those suppliers that were previously rated as critical or high because of data or transaction sensitivity will still be rated as critical or high. Factoring in the threat of ransomware to supplier operations, you will be adding a whole herd of suppliers to that critical or high tier.

Insight 3: Ensure that your operationally important suppliers have 24x7 security operations

Criminals are detonating ransomware seven days a week, with no day of the week having less than 12% of the total events. The data shows that criminals lean a bit towards detonating ransomware on the weekend, with 30% of all ransomware being detonated on Saturday or Sunday. Why do criminals favor the weekends? Perhaps because they know that the cybersecurity and IT teams of many organizations are understaffed, giving them more time to increase their attack blast radius.



We certainly have many examples in which the harm of ransomware was contained by the rapid response and good work of capable professionals. A prime example among many was that of Jackson Hospital, based out of Florida, in which their IT lead's rapid response to a ransomware event contained what could have otherwise been a devastating incident (https://www.cnn.com/2022/01/16/politics/florida-hospital-ransomware/index.html).

Ensure that your operationally important suppliers have 24x7 security operations. Rapid response to a ransomware event is essential to limiting data and getting on with recovering systems.

Insight 4: Don't assume recent ransomware victims materially improve their cybersecurity programs

Having been a cybersecurity practitioner for 25 years now, I have been around long enough to collect a few unfounded industry anecdotes. One of those that has been oft-repeated is, "The most secure company is the one that recently was breached." The reasoning was that companies that recently experienced a material breach would naturally make the investments necessary to strengthen their security program to minimize the likelihood of such an event occurring again.

That tale isn't true. Based on our analysis of the cybersecurity hygiene of victims of destructive ransomware attacks on the day of the attack compared with the cybersecurity hygiene of the same companies one year later, there is not much observable improvement. On average, a year after the event, many of the same and new critical software vulnerabilities are present in victim environments, unsafe network services remain invitingly open for criminals to compromise, and the communications encryption of many sensitive systems remain insecurely configured.

Table: Change in Cybersecurity Conditions in Internet-facing Systems
At Time of Ransomware Detonation Compared with One Year Later

	Day of Ransomware Event		One Year Later	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of Medium or higher (7.0 – 10)	percent with critical issues	56%	49%	12% better
	average issue count	13	11	15% better
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	percent with critical issues	32%	48%	50% worse
	average issue count	4	6	50% worse
Application Security Issues Missing common security practices in applications that collect sensitive data	percent with critical issues	53%	55%	4% worse
	average issue count	8	12	50% worse
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	percent with critical issues	72%	70%	3% better
	average issue count	45	46	2% worse
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	percent with critical issues	67%	58%	13% better
	average issue count	11	9	18% better

So, don't assume that a recent victim of ransomware is getting their cybersecurity house in order. The data doesn't bear it out. Looking at it on an industry level, half of the industries have worse cybersecurity hygiene one year after a ransomware event. As a risk practitioner, stick to your program. Stay after all the companies in your portfolio. Perhaps for those companies who have had a recent event, you should increase your assessment depth and frequency for multiple years.

Insight 5: Settle in for the long haul, the threat of ransomware is here to stay

Yes, I am stating the obvious; the threat of ransomware is here to stay. According to the stats from the U.S. Treasury Department, U.S. victims of ransomware paid $590 million in ransom to ransomware criminals in the first half of 2021 (https://home.treasury.gov/news/press-releases/jy0471). That big money has attracted a lot of ransomware gangs. Reporters covering the ransomware beat identified 59 different criminal groups behind the attacks over the last three years.

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 program, as they are the basics of managing IT and cybersecurity well. It is just that it is now more important to ensure your suppliers are doing the basics well.

Coveware's 2021 ransomware study reinforces the importance of doing the basics well. Among other gems, they found that 42% of ransomware events started with a phishing attack, 42% exploited the environment through an internet-exposed RDP or another remote management service, and 14% exploited a software vulnerability present in an internet-facing system. Those three vectors accounted for 98% of ransomware attacks – the basics! (https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/).

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. In this section, I call out a few key controls that are commonly cited in reputable sources and standards that you should consider adding to your supplier assessment criteria. For a complete set of recommendations, I suggest reading the sources provided at the end of this section.

1) Operate an effective backup and restoration program.

- Make regular backups of all data files necessary to restore business operations in the face of loss of systems, applications, and data.
- Periodically restore systems from backup to ensure that backups are sufficient to restore operations quickly.
- Create offline backups that are separate from online backups to guard against the event that the ransomware reaches backup systems.

2) Prepare for an incident.

Verify that suppliers have a documented and practiced incident response plan and that they have a ransomware-specific response playbook.

3) Educate employees on how to identify and respond to phishing emails.

Cited earlier, 42% of ransomware attacks start with phishing. Ensure that suppliers are educating their personnel regarding the risk of phishing attacks and how to avoid becoming a victim. Employee security awareness companies such as KnowBe4, PhishMe, and Proofpoint, among others, actively engage employees in training programs with great results.

4) Only expose authorized and hardened network services to the Internet.

Sharing the lead with phishing, 42% of ransomware attacks start with exploiting an internet-accessible Remote Desktop Protocol Service. RDP services become more prominent during the pandemic as companies often hastily migrated employees to remote work.

Regardless of whether it is an employee's computer operating from home, or a server deployed in a data center or the cloud, ensure that suppliers restrict all internet-exposed network services to only those that are explicitly authorized and that are operated in a defensible manner. RDP, a very common and commonly exploited remote access service, should not be exposed to the Internet. Rather, a secure VPN service should be used that requires two-factor authentication.

5) Keep software patches current.

According to Coveware, 14% of ransomware attacks started with exploiting vulnerable software in an internet-facing system. Demand that your suppliers operate a robust program for keeping software patches current, particularly the software of internet-facing systems.

6) Prevent malware from being delivered and spreading to devices

- Filter malicious emails before delivery to mailboxes for malicious software, phishing content, and disreputable sources.
- Proxy all end-user Internet traffic through a proxy that automatically blocks access to malicious sites and dynamically detects and blocks malicious code and content. A stronger approach to protecting against web-native threats is allowing access to only safe browsing lists.

7) Prevent malware from running on devices

An ideal position to be in is one in which malware simply can't operate on endpoints. Suppliers can get part of the way there with endpoint protection platforms on every system. These stop identified threats before they install on the host system. However, they don't provide 100% protection.

Two additional controls will greatly enhance the defensibility of systems.

- Remove administrator privileges from users and applications. This single action will render most ransomware from successfully operating on patched systems.
- Centrally administer systems and control what software can be installed and operated on systems. Application allow-list solutions can help manage this at scale.

8) Detect malicious network and endpoint activity

Of course, it is unreasonable to expect that the preventitive controls will block all threats. As such, it is essential to have robust network and endpoint activity and threat monitoring and blocking. This includes monitoring for intrusion attempts, sourcing from both outside and inside the network, data exfiltration attempts, known malicious, and abnormal communications.

A few resources from which these recommendations were developed and provide deeper treatment of ransomware defense are:

- The UK National Cyber Security Centre - https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- From Google - https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks
- Carnegie Mellon University's Software Engineering Institute - https://insights.sei.cmu.edu/blog/ransomware-best-practices-for-prevention-and-response/
- The Cybersecurity and Infrastructure Security Agency - https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Conclusion

No company can operate well without its suppliers delivering the goods and services reliably. Ransomware threatens the operations of nearly every vendor in your 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 destructive 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 can't outsource your risk. RiskRecon helps you achieve better supply chain risk outcomes at scale.

About RiskRecon

RiskRecon, a Mastercard Company, 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.