# Five lessons from 1,000 destructive ransomware events

## Managing the risk of ransomware in the supply chain

## January 2023

riskrecon.com

sales@riskrecon.com

© Copyright 2023

# Introduction

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 robust resilience measures in place. Unfortunately, as we have learned in the face of other threats, this is not the case.

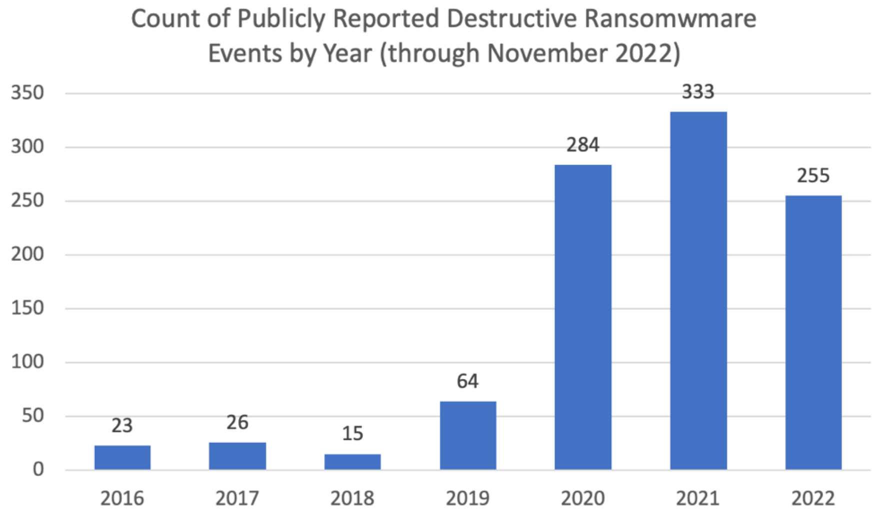
The reality of uneven cyber security strength in the supply chain leaves risk managers to answer critical questions for the enterprise. How resilient is my supply chain to ransomware? Which of my hundreds of suppliers represent the greatest risk? What should I do to address the risks? Perhaps the most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

Managing 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 1,000 publicly disclosed ransomware events occurring between January 2016 and November 2022.

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 show they make only marginal improvements 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 1,000 publicly reported destructive ransomware events that occurred between January 2016 and November 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.



RiskRecon limited ransomware events included in the study that impacted operations due to the encryption of systems. Destructive ransomware is particularly interesting because disrupting operations requires the deep compromise of an organization – the initial foothold, pivoting around the network to find operationally sensitive systems, and then detonation.

For each event, RiskRecon assessed the cybersecurity hygiene of each victim on the date of ransomware detonation and during the months and years following using its cybersecurity ratings platform through which RiskRecon continuously monitors the cybersecurity hygiene of over 5 million organizations. RiskRecon's assessments are based on a passive assessment of nine security domains and 33 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.

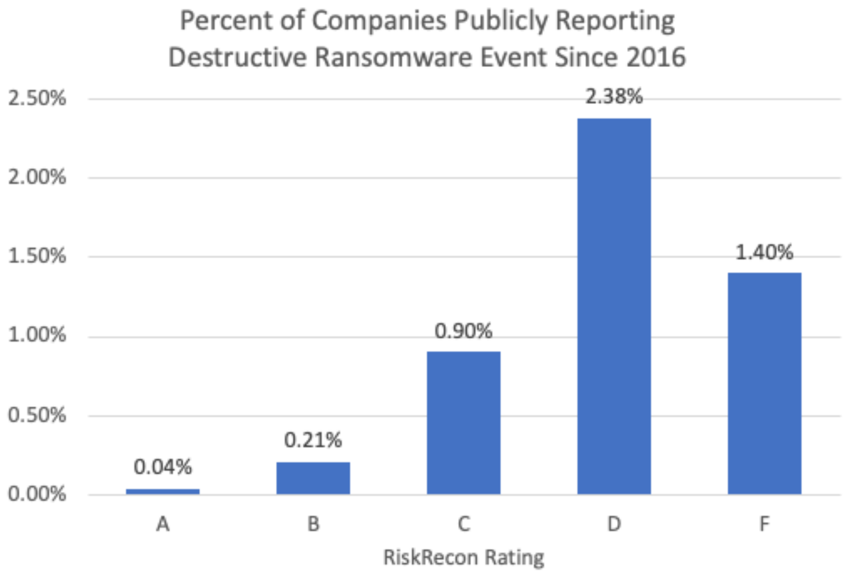
## Lesson 1: Do business with suppliers that have good cybersecurity hygiene

Based on RiskRecon's comparison population of nearly 180,000 organizations, those that RiskRecon observes to have very poor cybersecurity hygiene in their Internet-facing systems (a 'D' or 'F' RiskRecon rating) have a 50 times higher rate of destructive ransomware events in comparison with companies that have clean cybersecurity hygiene. As shown in the chart below, only 0.04% of 'A-rated' companies were victims of a destructive ransomware attack, compared with 2.38% of 'D-rated' and 1.40% of 'F-rated' companies.

**Organizations with good cybersecurity hygiene have a**

**50x lower**

**frequency of destructive ransomware events**



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 180,000 companies, those that succumb to destructive ransomware, on average, have:

- 11 times higher and more critically severe issues 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 has HTTP encryption issues such as expired certificates, weak encryption algorithms, or invalid certificate subjects.

The table below compares the count of cybersecurity hygiene issues existing in the internet-facing systems of ransomware victims at the time of detonation with the general population across seven security domains.

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

| | Average Issue Count | | |
|---|---|---|---|
| | **Ransomware Victim** | **General Population** | **Difference** |
| **Software Patching Issues**<br>Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10) | 21.3 | 1.9 | 11x higher |
| **Unsafe Network Services**<br>Internet-exposed unsafe services such as databases and remote administration | 23.0 | 4.3 | 5.3x higher |
| **Application Security Issues**<br>Missing common security practices in applications that collect sensitive data | 16.6 | 2.1 | 7.9x higher |
| **Web Encryption Issues**<br>Errors in encryption configuration in systems that collect and transmit sensitive data | 35.0 | 3.8 | 9.2x higher |
| **Email Security Issues**<br>Security issues in active email servers and domains that increase susceptibility to phishing and data theft | 7.6 | 1.3 | 5.8x higher |
| **System Reputation Issues**<br>Number of systems exhibiting malicious activity such as communicating with botnet controllers, block-listed for attempting to compromise other systems or spamming. | 9.0 | 1.0 | 9x higher |

Ignoring issue counts and just looking at the percentage of companies with one or more issues across the cybersecurity domains, the ransomware victim group again stands out as having very poor hygiene in comparison to the general population. In comparison with the general population, the population of companies that have succumbed to ransomware has:

- 3.2 times more companies with at least one high or critically severe software vulnerability in their internet-facing systems.
- 1.8 times more companies with at least one unsafe network service exposed to the internet.
- 5.5 times more companies with at least one system exhibiting malicious activity such as botnet communications.
- 1.9 times more companies with at least one sensitive web application 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**<br>Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10) | 57% | 18% | 3.2x higher |
| **Unsafe Network Services**<br>Internet-exposed unsafe services such as databases and remote administration | 53% | 29% | 1.8x higher |
| **Application Security Issues**<br>Missing common security practices in applications that collect sensitive data | 45% | 37% | 1.2x higher |
| **Web Encryption Issues**<br>Errors in encryption configuration in systems that collect and transmit sensitive data | 75% | 39% | 1.9x higher |
| **Email Security Issues**<br>Security issues in active email servers and domains that increase susceptibility to phishing and data theft | 65% | 36% | 1.8x higher |
| **System Reputation Issues**<br>Number of systems exhibiting malicious activity such as communicating with botnet controllers, block-listed for attempting to compromise other systems or spamming. | 11% | 2% | 5.5x higher |

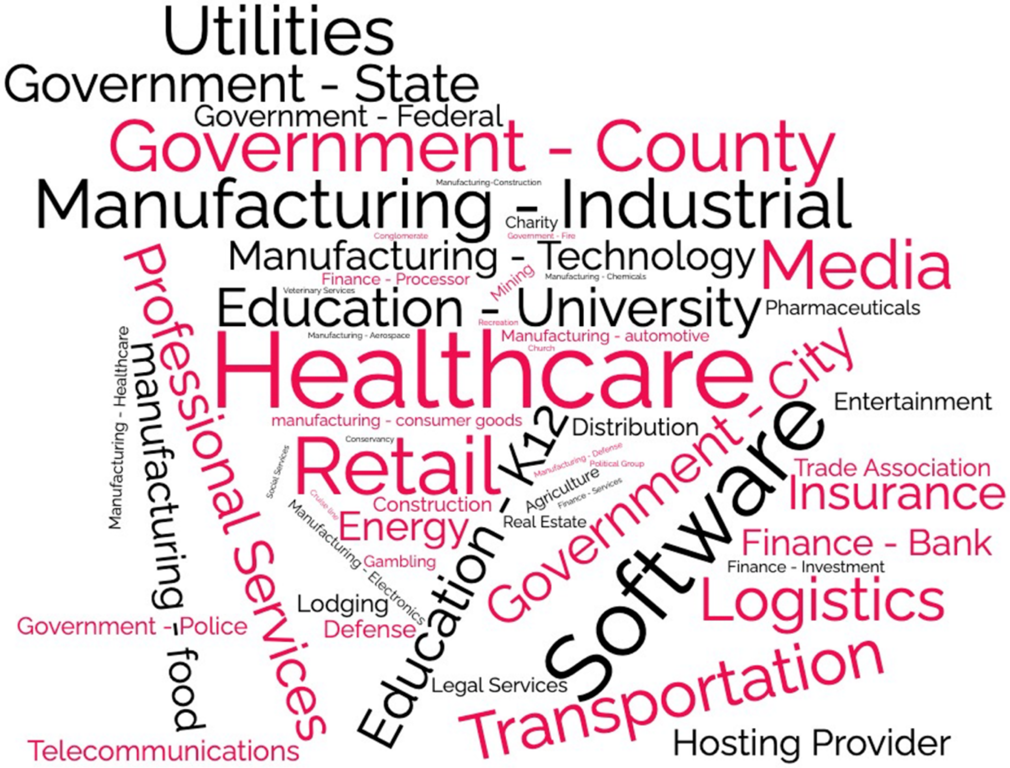
Why is there such a strong correlation between cybersecurity hygiene and ransomware event frequency? Detonating system encrypting ransomware within the systems that will materially harm the operations is not trivial if security shields are up. First, the criminals must gain an initial foothold in the 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.

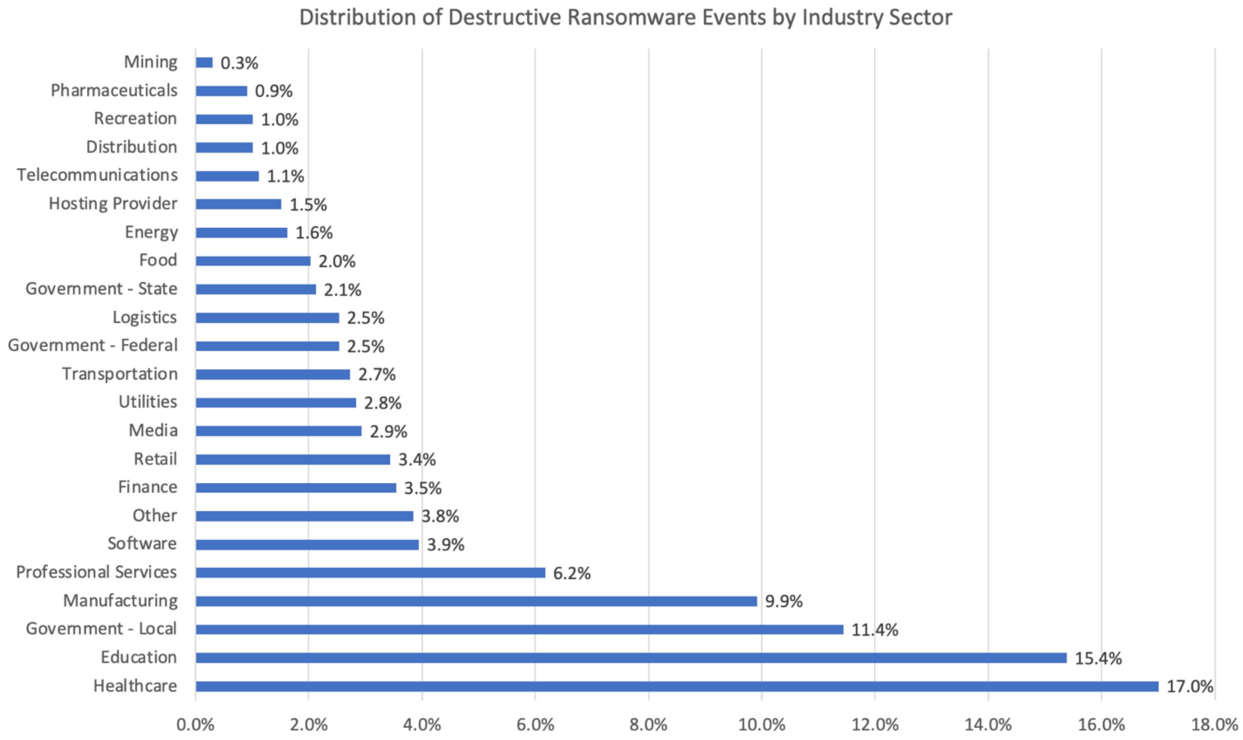
## Lesson 2: Revisit your supplier inherent risk ratings; criminals are targeting everyone

In the pre-ransomware world, vendor inherent risk rating models were weighted primarily toward dimensions such as spend, data types, transaction types, and related volumes. This 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.

Across the 1,000 events spanning January 2016 to November 2022, criminals disrupted the operations of organizations across 56 different industry sub-sectors. The word cloud below shows the breadth and focus of attacks. We are talking about ransomware being detonated in industries from mining to food manufacturing, from fire departments to financiers, and from churches to elementary schools. Even veterinary clinics succumbed to ransomware.



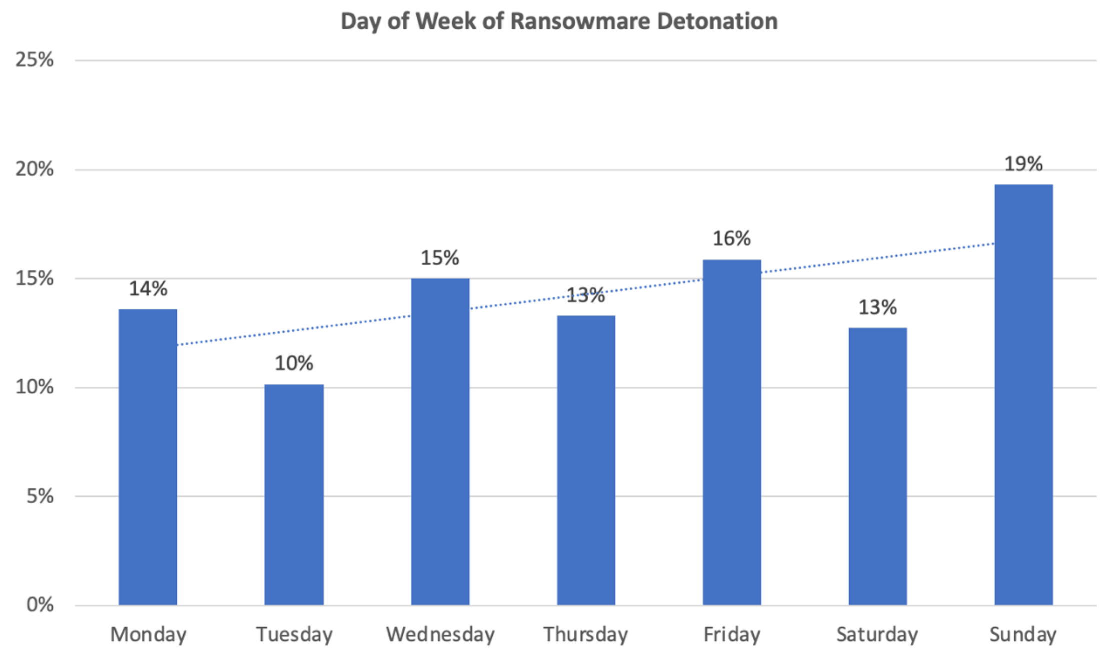
Unfortunately for all of society, healthcare providers have suffered 17% of all destructive ransomware events, rendering hospitals and clinics inoperable in geographies ranging from Japan to Germany. Education has struggled to keep control of its systems, accounting for 15.4% of all events, split 60/40 between K-12 and Universities. Local governments round out the top three, accounting for 11.4% of all destructive ransomware events, with city governments bearing most of the load at 68% of all local government attacks.



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 bunch more to that critical or high tier.

## Lesson 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 10% of the total events. Be certain to have coverage through the long weekend. Forty-eight percent of all ransomware detonation occurs Friday – Sunday. Why do criminals favor the weekends? Perhaps because they know that organizations have fewer cybersecurity and IT professionals at the ready during the weekend, giving them more space to increase their blast radius.



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

## Lesson 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.

The reality is that one year after a destructive ransomware event, many companies do improve significantly, with many eliminating all issues in their internet-facing systems. However, we do see many degrade in the areas of unsafe network services and email security. Importantly, their cybersecurity hygiene continues to significantly lag behind that of the general population.

Comparing ransomware victim cybersecurity hygiene one year after with their hygiene on the day of detonation we see some improvements and, sadly, some degradation. Looking at the change in average issue count:

- The average count of critical or high software vulnerabilities decreases by 15%.
- The number of unsafe network services increases by 69%.
- The volume of malicious communications to the internet decreases by 8%.
- The number of sensitive web applications decreases by 31%.

**Table:** Comparison of the count of security issues in internet-facing systems on the day of detonation

| | **Average Issue Count** | | |
|---|---|---|---|
| | **Day of Detonation** | **One Year Later** | **Change** |
| **Software Patching Issues**<br>Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10) | 21.3 | 13.7 | 36% better |
| **Unsafe Network Services**<br>Internet-exposed unsafe services such as databases and remote administration | 23.0 | 39.0 | 69% worse |
| **Application Security Issues**<br>Missing common security practices in applications that collect sensitive data | 16.6 | 9.2 | 45% better |
| **Web Encryption Issues**<br>Errors in encryption configuration in systems that collect and transmit sensitive data | 35.0 | 24.1 | 31% better |
| **Email Security Issues**<br>Security issues in active email servers and domains that increase susceptibility to phishing and data theft | 7.6 | 8.5 | 12% worse |
| **System Reputation Issues**<br>Number of systems exhibiting malicious activity such as communicating with botnet controllers, block-listed for attempting to compromise other systems or spamming. | 9.0 | 8.3 | 8% better |

The situation looks quite a bit brighter when looking at the percentage of companies with one or more issues across the assessed security domains.

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

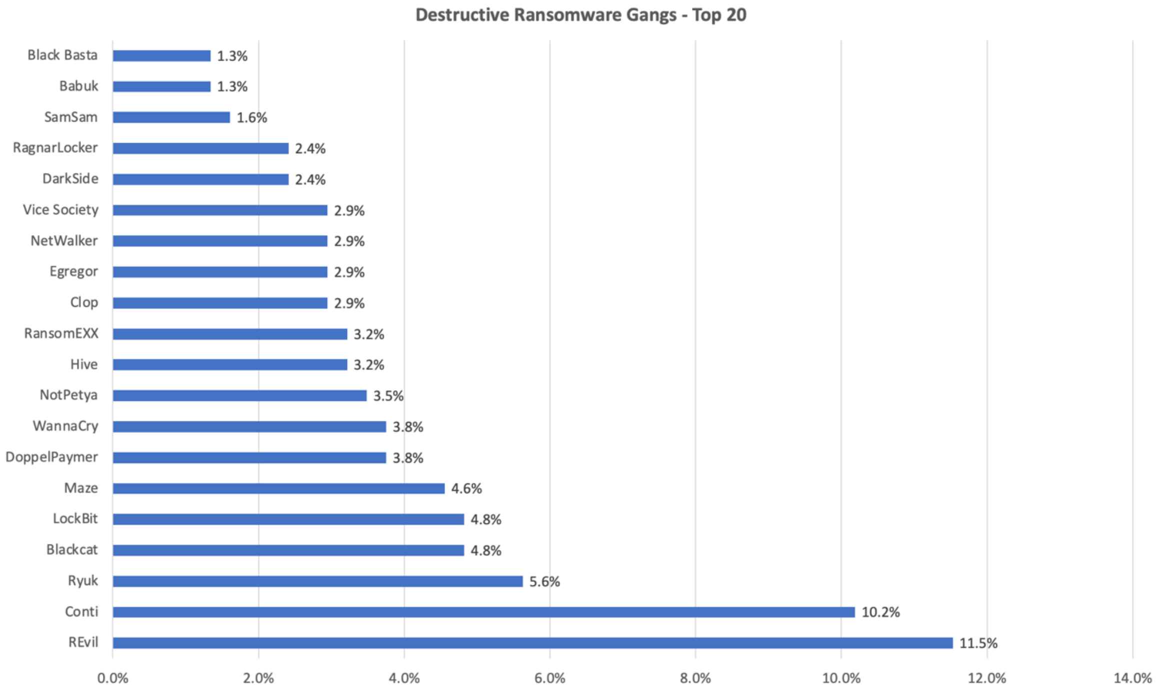
| | **Percent with at Least One Issue** | | |
|---|---|---|---|
| | **Day of Detonation** | **One Year Later** | **Change** |
| **Software Patching Issues**<br>Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10) | 57% | 30% | 44% better |
| **Unsafe Network Services**<br>Internet-exposed unsafe services such as databases and remote administration | 53% | 35% | 34% better |
| **Application Security Issues**<br>Missing common security practices in applications that collect sensitive data | 45% | 32% | 29% better |
| **Web Encryption Issues**<br>Errors in encryption configuration in systems that collect and transmit sensitive data | 75% | 72% | 4% better |
| **Email Security Issues**<br>Security issues in active email servers and domains that increase susceptibility to phishing and data theft | 65% | 64% | 2% better |
| **System Reputation Issues**<br>Number of systems exhibiting malicious activity such as communicating with botnet controllers, block-listed for attempting to compromise other systems or spamming. | 11% | 11% | no change |

While the data show that many victims of destructive ransomware improve their cybersecurity hygiene, many do not. The smart move would be to dig into companies that have been breached and stay after them to ensure that they implement plans to reduce the likelihood and impact of a future breach.

## 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. banks processed about $1.2 billion in ransomware-related payments on behalf of their clients in 2021 (https://www.cnbc.com/2022/11/01/us-banks-process-roughly-1point2-billion-in-ransomware-payments-in-2021.html). That big money has attracted a lot of ransomware gangs. Reporters covering the ransomware beat identified 67 different criminal groups behind the attacks over the last six years.

Avaddon
WastedLocker
Ryuk
Astro
Snake
DarkSide
Deadbolt
WannaCry
Hive
Quantum
Trickbot
ShinyHunters
Belarusian Cyber Partisans
DoppelPaymer
Hades
Team Johnwick
Snatch
HelloKitty
SYNack
Nefilim
Grief
AvosLocker
Anonymous
NB65
Pay2Key
Defray
Pysa
LV
REvil
Conti
Maze
Calix
Gallium
Lorenz
SamSam
LAPSU$
m1x
ShinyHunters
Ragnar Locker
Pandora
Qbot
LockBit
DonJuj
AnarchyGrabber
Rick Rollers
Sodinokibi
Blackcat
SunCrypt
cuba
Black Basta
Dharma
Vice Society
RansomHouse
Cozy Bear
Egregor
RagnarLocker
NotPetya
CryptoLocker
Clop
NetWalker
xing team
Blackbyte
BlackMatter
Babuk
RansomEXX
Powerful Greek Army
Phoenix CryptoLocker



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 than ever to ensure your suppliers are doing the basics well.

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.

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.

According to Coveware's Q2 2022 ransomware report[1], 35% 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, 30% of ransomware attacks start by exploiting an internet-accessible Remote Desktop Protocol Service[2]. RDP and other remote access services have become more pervasive to support remote work. Many deployed those services insecurely.

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 require two-factor authentication.

5) Keep software patches current.

According to Coveware, 20% of ransomware attacks started by exploiting vulnerable software in an internet-facing system[3]. 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.

[1] https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

[2] https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

[3] https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

- 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 preventive 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, and 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 and https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

## 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.