The 2024 state of ransomware

Five lessons for TPRM professionals

WHITE PAPER

APRIL 2024

Contents

3 Introduction

5 The Study

6 Lesson 1: Do business with organizations that have good cybersecurity hygiene

10 Lesson 2: Revisit your suppliers' inherent risk ratings; criminals are targeting every sector

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

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

16 Lesson 5: Settle in for the long haul; the threat of ransomware is growing in volume and impact

21 Conclusion

Introduction

"In the span of eight years, RiskRecon has cataloged and analyzed 1,454 destructive ransomware events."

In the span of eight years, RiskRecon has cataloged and analyzed 1,454 destructive ransomware events, many of dramatically greater impact than these bookends. These include events that crippled the delivery of energy and utility services, forced shutdowns of numerous 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.

In 2016, RiskRecon by Mastercard analysts cataloged 22 destructive ransomware events, a subset of ransomware attacks that materially harm the victim's ability to operate by encrypting critical systems. The first occurred on Monday, January 25, 2016, against the Israel Electric Authority. Though it forced the shutdown of many systems, it did not impact the generation or transmission of electricity. In 2023, RiskRecon analysts recorded 373 destructive ransomware events, the last detonating on Tuesday, December 26, 2023, in the systems of the Government of Trinidad and Tobago's social security agency, forcing a multi-day closure of services.

The details of these destructive ransomware events contain valuable lessons for better managing enterprise cybersecurity risks for the enterprise and the supply chain. Even if one's own cybersecurity house is in a great position, 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 research team has distilled five important insights for managing supply chain risk from these 1,454 destructive ransomware events. These same lessons apply equally to one's own enterprise cybersecurity risk posture.

1. Do business with organizations that have good cybersecurity hygiene; they have dramatically lower rates of destructive ransomware and data loss events.

2. Revisit your suppliers' inherent risk ratings to include operational dependency; criminals are targeting every sector.

3. Ensure that your operationally important suppliers have 24x7 security operations; criminals are detonating ransomware seven days a week.

4. Don't assume recent ransomware victims materially improve their cybersecurity program; the data shows they make only marginal improvements in their cybersecurity hygiene one year after an event.

5. Shore up your cybersecurity risk management programs; the threat of ransomware is growing in volume and impact.

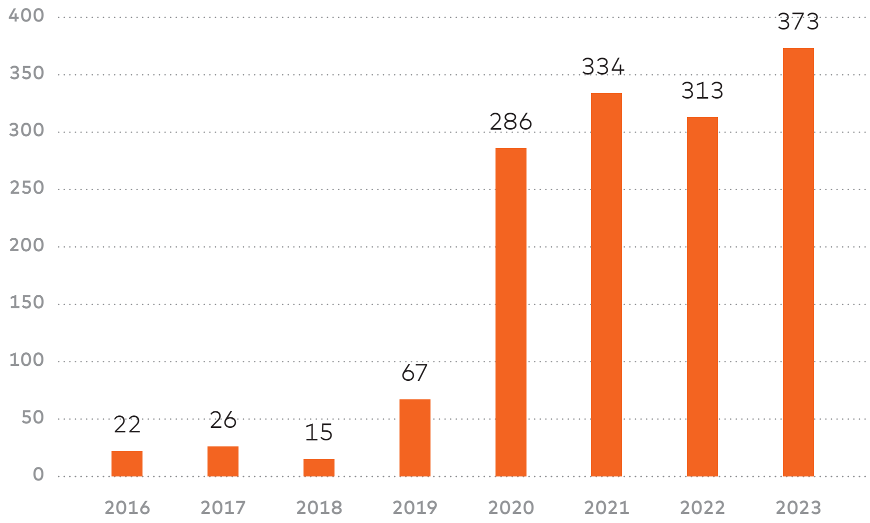
We all have a shared responsibility in managing the risk of ransomware because no enterprise exists in isolation. Perhaps one of the greatest services that a cybersecurity team can render after ensuring their own house is in order is to help their suppliers and partners protect their houses. As is always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

The study

"Criminals had to compromise an organization deep enough to pivot around the infrastructure to discover and compromise operationally sensitive systems."

RiskRecon cataloged and studied 1,454 publicly reported destructive ransomware events between January 2016 and December 2023. These events were identified through internet keyword searches, monitoring of event disclosure sites, dark web sites, and 8K Securities and Exchange Commission (SEC) filings. We excluded events where the impact was limited to data theft.

Count of destructive ransomware events by year tracked by RiskRecon



This study is focused on destructive ransomware events in which the victim's ability to operate was materially impacted due to the encryption of critical systems. These are a subset of all reported ransomware events, which have swelled to include almost all outside threat actor system compromises. Destructive ransomware events contain valuable lessons because, in these incidents, criminals had to compromise an organization deep enough to pivot around the infrastructure to discover and compromise operationally sensitive systems before detonation.

For 817 of the events, RiskRecon had cybersecurity ratings and assessment data for the impacted companies in its platform surrounding the date of the ransomware detonation and during the time that followed the incident. RiskRecon's assessments are based on a passive assessment of nine security domains and 33 security criteria spanning thousands of security checks. RiskRecon's assessments cover software patching, application security, web encryption, network filtering, and so forth. RiskRecon distills each assessment, detailing the I.T. profile, the security issues, and related severities, into a simple cybersecurity rating of A to F, with A being the best.

LESSON

01

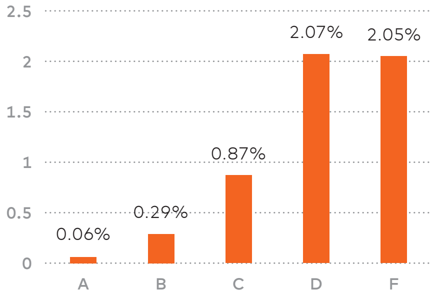
Do business with organizations that have good cybersecurity hygiene

Looking across RiskRecon's population of 150,000 analyst-supervised organizations, those with very poor cybersecurity hygiene, rated as D or F, have experienced a 35x higher frequency of breach events compared to A-rated organizations, which RiskRecon observes as having very clean hygiene. Just over 2% of D and F-rated companies have had a destructive ransomware event since 2016. In comparison, only 0.06% of A-rated companies and 0.29% of B-rated companies have suffered a destructive ransomware event.

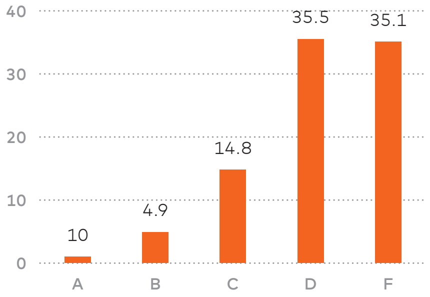
35x

Organizations with good cybersecurity hygiene have a 35 times lower frequency of destructive ransomware events

Destructive ransomware event frequency by rating

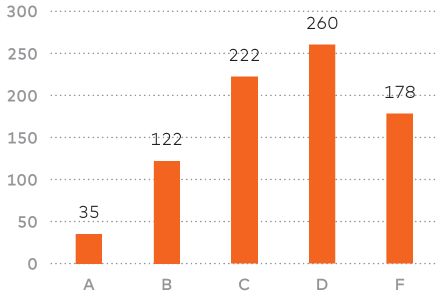


Destructive ransomware event frequency relative to A rated orgs

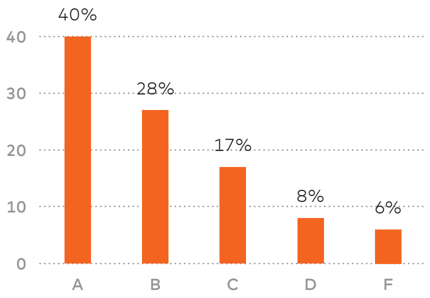


Lest one think that the larger populations of A and B-rated organizations are skewing the correlation; A and B-rated organizations have the lowest and second lowest count of ransomware events. Of the 817 events for which RiskRecon had ratings of the organization surrounding the time of detonation, only 35 were A-rated, while D-rated organizations had the highest event count at 260. Graphs showing event counts by rating and the distribution of the 150,000 companies are below.

Count of destructive ransomware events by rating



Global population ratings distribution



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 destructive ransomware, on average, have:

- 7.2 times more high and critical severity issues in their internet-facing systems
- 12.2 times more unsafe network services exposed to the internet, such as Remote Desktop Protocol (RDP), telnet, database listeners, NetBIOS, and SMB
- 23.7 times higher rate of malicious activity, such as botnet communications, emanating from their systems to the internet
- 6.4 times higher frequency of encryption configuration issues in high-value systems that collect and transmit sensitive data
- 5.2 times higher rate of email server security configuration issues

Table: Comparison of the count of security issues in internet-facing systems surrounding the 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)	29.4	4.1	7.2x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	20.8	1.7	12.2x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	19.1	2.6	7.3x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	38.3	6	6.4x higher
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	14.6	2.8	5.2x 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	7.1	0.3	23.7x higher

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

- 2.4 times more organizations with at least one high or critical severity software vulnerability in their internet-facing systems
- 2.1 times more organizations with at least one unsafe network service exposed to the internet
- 5.3 times more companies with at least one system exhibiting malicious activity, such as botnet communications
- 2.1 times more companies with at least one web application that transmits sensitive data with 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 1 Issue		
	Ransomware Victim	**General Population**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	58%	24%	2.4x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	54%	26%	2.1x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	58%	38%	1.5x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	76%	36%	2.1x higher
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	59%	29%	2.0x 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	16%	3%	5.3x higher

"Nearly 48% of the initial attack ingress vectors were either exploiting unpatched software or unsafe network services — basic cybersecurity hygiene practices."

This powerful correlation between ransomware frequency and RiskRecon's observed cybersecurity hygiene is substantiated by Coveware's findings in its quarterly ransomware report, based on its first-responder ransomware recovery work. From 2020 through 2023, nearly 48% of the initial attack ingress vectors were either exploiting unpatched software or unsafe network services — basic cybersecurity hygiene practices.[1]

Why such a strong correlation? If security shields are up, detonating systems encrypting ransomware within operationally sensitive systems is not trivial. First, the criminals must gain an initial foothold in the environment. Then, the criminals must pivot around the network to identify and compromise a system or systems that will impact operations. Finally, they can trigger an impactful detonation.

Organizations with poor security hygiene in their external surfaces provide easy initial entry vectors and are unlikely to have strong internal defenses that reduce the risk of ransomware detonation. Conversely, organizations that demonstrate very clean hygiene in their externally observable systems and signals don't offer as many initial entry vectors and are more likely to have strong internal defenses. There is no guarantee, but it is definitely more likely.

[1] https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

LESSON

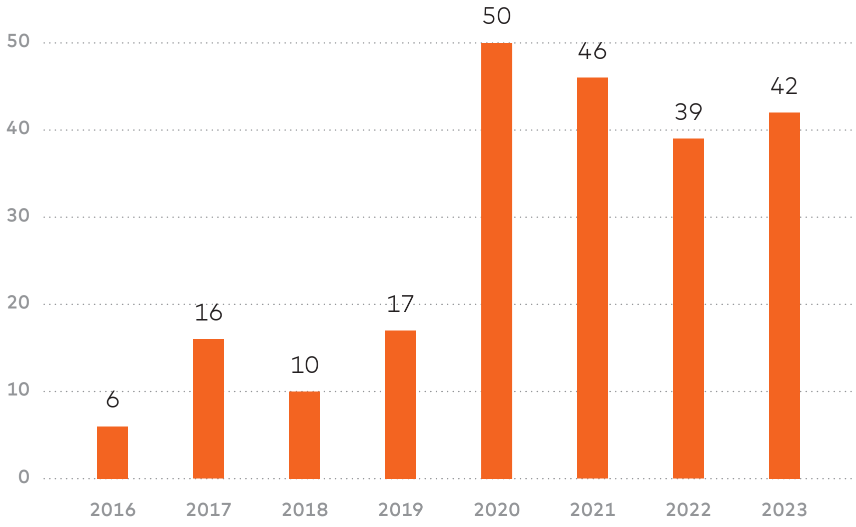
02

Revisit your suppliers' inherent risk ratings; criminals are targeting every sector

Across the 1,454 destructive ransomware events, spanning January 2016 to December 2023, criminals disrupted the operations of organizations across 64 different industry sub-sectors. In 2016, just a few industries were hit, primarily utilities, healthcare, and national governments. As 2023 closed out, the victim list had expanded to include casinos, hotels, local fire and police departments, agriculture, and even cruise lines. Even veterinary clinics succumbed to ransomware.

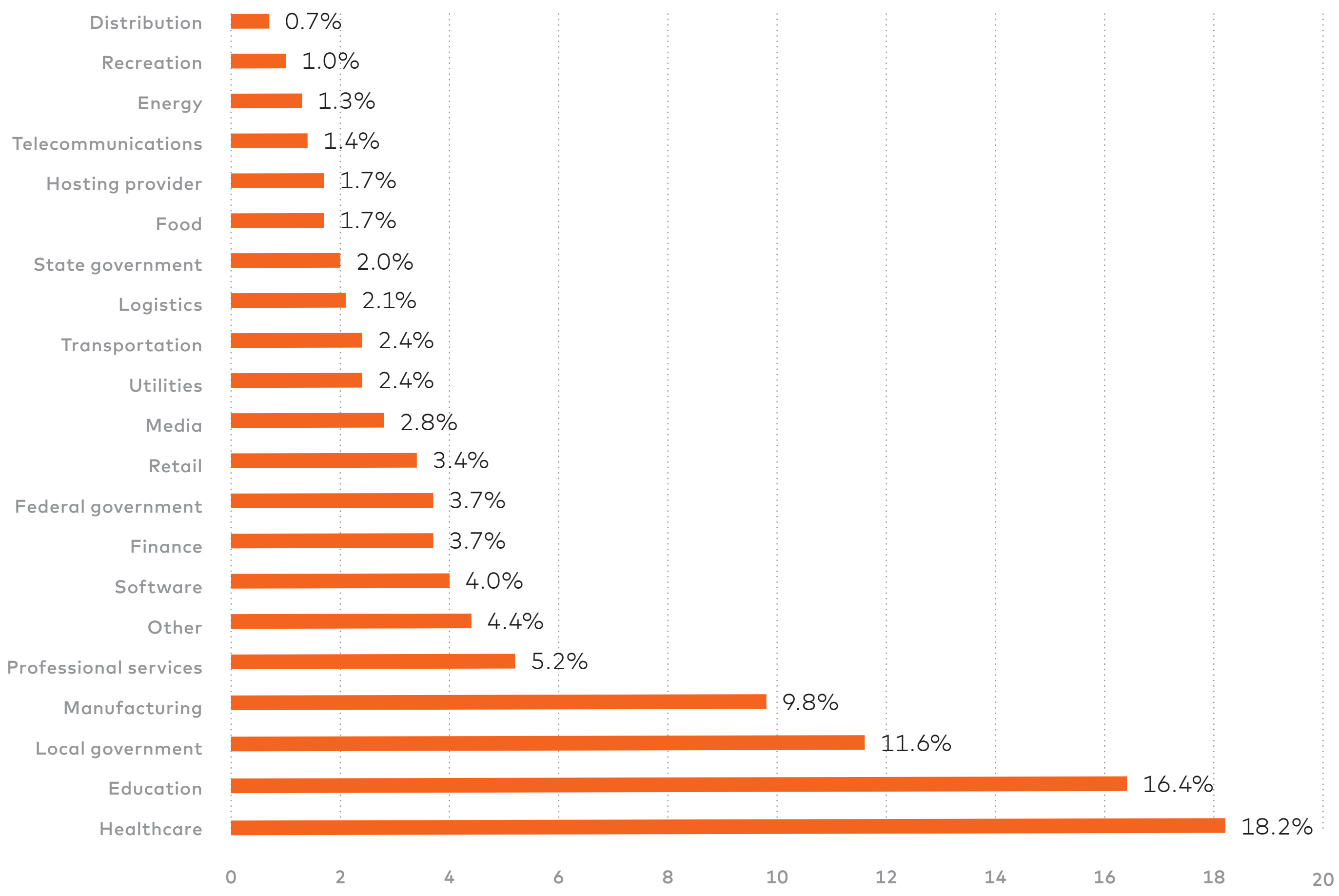
"As 2023 closed out, the victim list had expanded to include casinos, hotels, local fire and police departments, agriculture, and even cruise lines."

Industries hit by destructive ransomware by year



Unfortunately for society, healthcare providers have been the most frequent victims, accounting for more than 18% of all destructive ransomware events, rendering hospitals and clinics inoperable in geographies ranging from Japan to Germany. Education has struggled to control its systems, accounting for 16.4% of all events, split 60/40 between K-12 and universities. Local governments round out the top three, accounting for 11.6% of all destructive ransomware events.

Distribution of destructive ransomware events by industry sector



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. Every vendor and partner is a likely 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 actually be high or critical when examined through the lens of operational dependency.

LESSON

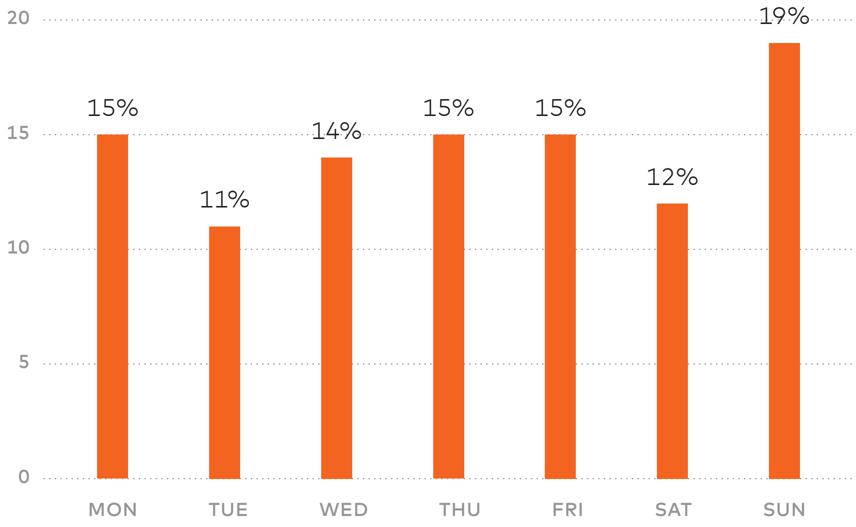
03

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 11% of the total events. Be certain to have coverage through the long weekend, where 46% of all ransomware detonations occur from Friday to Sunday. Why do criminals favor the weekends? Perhaps because they know that organizations have fewer cybersecurity and I.T. professionals at the ready during the weekend, giving them more space to increase their blast radius.

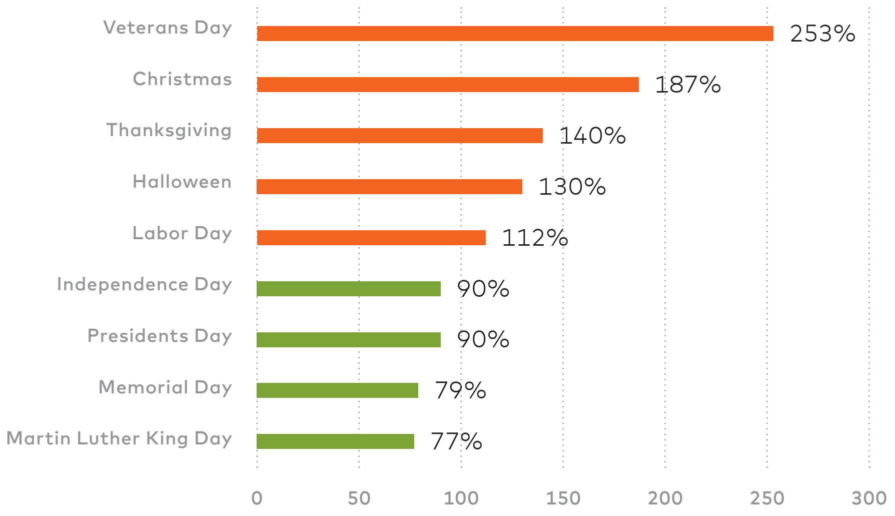
"46% of all ransomware detonations occur from Friday to Sunday."

Day of week destructive ransomware detonated



Borrowing from our broader study of nearly 9,000 data breach events occurring from 2012 to 2021 — the data shows that criminals aren't resting on the major U.S. holidays either. Throughout the 10-year span of the study, five of the nine holiday windows had a higher breach event rate than the daily average. The days surrounding Veterans Day had the highest holiday-related breach event frequency, running at 253% above average. Christmas and Thanksgiving also ran hot at 187% and 140% above average. Surprisingly, the big U.S. vacation windows of Independence Day, Labor Day, and Memorial Day ran below average.

Holiday window percent of average daily breach event rate 2012–2021



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

LESSON

04

Don’t assume recent ransomware victims materially improve their cybersecurity programs

It would be reasonable to expect that an organization that had recently suffered a material breach of its business would allocate resources to shore up the security hygiene of its estate, including shutting down unsafe network services and eliminating material software vulnerabilities in its internet-facing systems. Unfortunately, the data doesn’t support that expectation.

Comparing ransomware victim cybersecurity hygiene one year after with their hygiene on the day of detonation, we see a minor improvement in some areas but, sadly, greater degradation in others. Looking at the change in average issue count:

- The average count of critical or high software vulnerabilities decreases by 8%
- The number of unsafe network services increases by 56%
- The volume of malicious communications to the internet increases by 17%
- The number of sensitive web applications with broken encryption increases by 3%

Table: Comparison of the count of security issues in the internet-facing systems of ransomware victims on the day surrounding detonation versus one year later

	Average Issue Count		
	Day of Detonation	One Year Later	Change
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	29.4	27.0	8% better
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	20.8	32.5	56% worse
Application Security Issues Missing common security practices in applications that collect sensitive data	19.1	17.8	7% better
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	38.3	39.7	3% worse
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	14.6	13.5	8% better
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	7.1	8.3	17% worse

The situation looks no better when looking at what percentage of ransomware victims have at least one issue in their internet-facing systems one year after detonation.

Table: Comparison of the count of security issues in the internet-facing systems of ransomware victims on the day surrounding detonation versus one year later

	Percent with at Least 1 Issue		
	Day of Detonation	One Year Later	Change
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	58%	55%	5% better
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	54%	58%	7% worse
Application Security Issues Missing common security practices in applications that collect sensitive data	58%	59%	2% worse
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	76%	72%	5% better
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	59%	65%	10% worse
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	16%	13%	19% better

Doing cybersecurity well is tough. It requires that systems be really well managed, which necessitates good people, processes, and supporting technology. All this starts with strong commitment from the top of the organization, backed by budget and prioritization to make it happen. A transformation like that doesn't happen easily. As we see in the data, one year later, ransomware victims aren't doing any better than when they first succumbed to the threat.

Based on this data, the smart move for vendor risk managers would be to really dig into companies that have suffered breaches and stay after them to ensure that they implement and sustain programs to reduce the likelihood and impact of a future breach.

LESSON

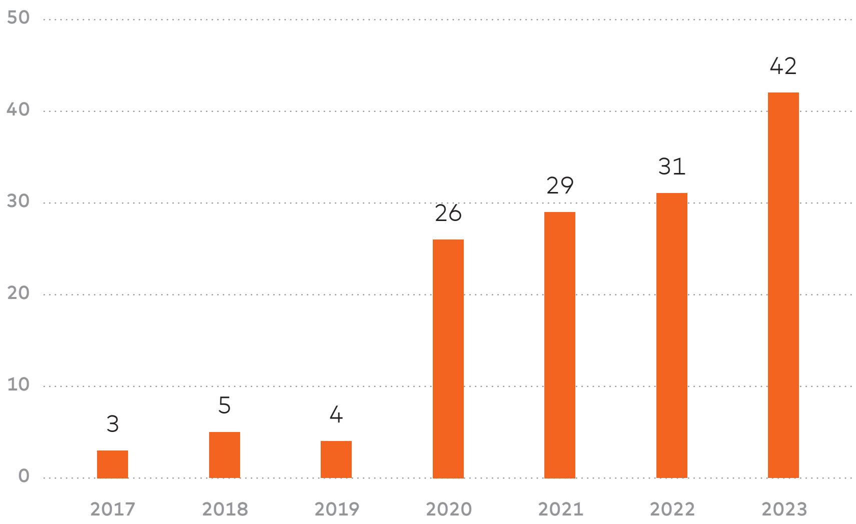
05

Settle in for the long haul; the threat of ransomware is growing in volume and impact

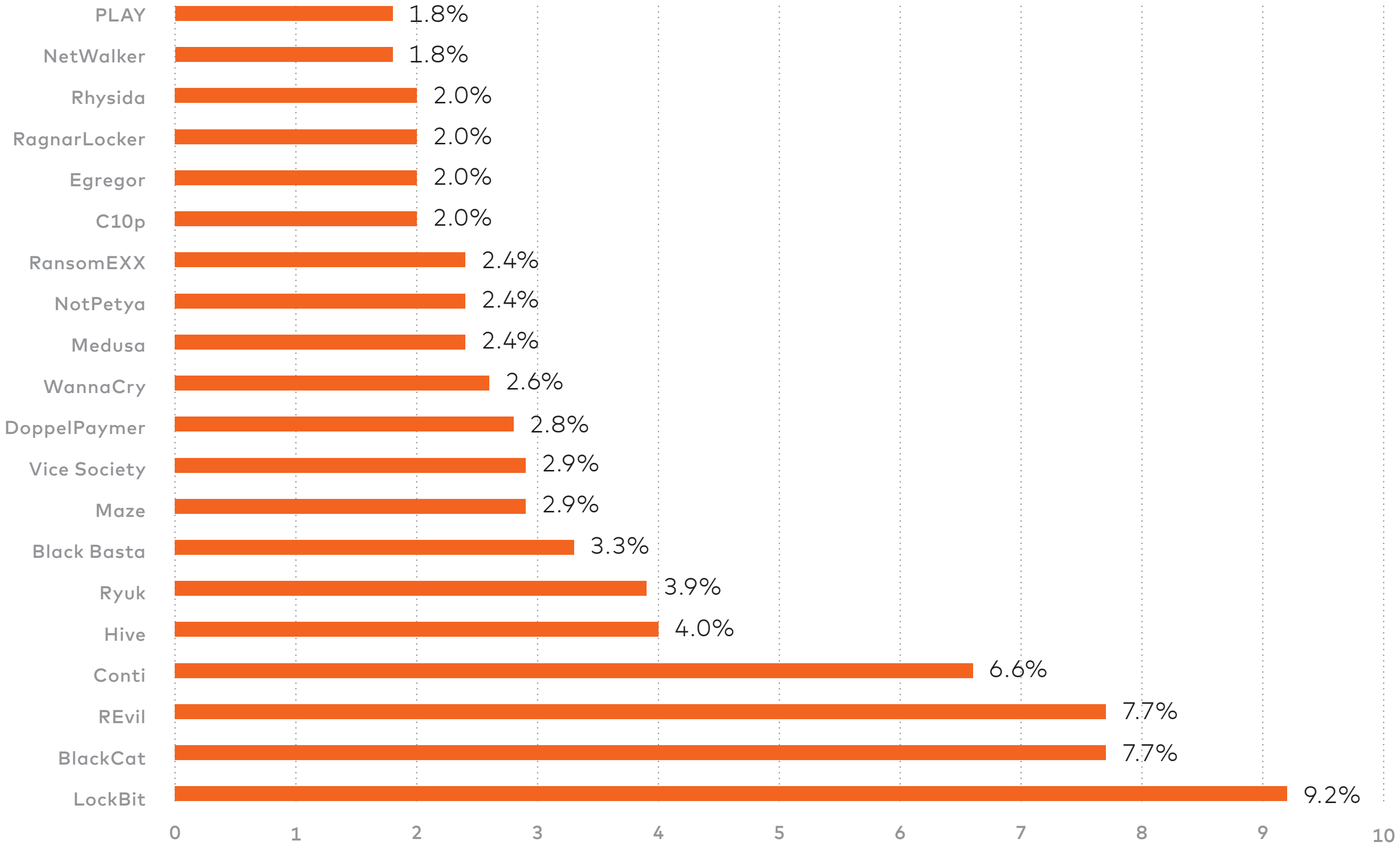
The amount of resources criminals are directing towards destructive ransomware attacks is growing dramatically. From 2017 through 2023, 92 different criminal groups were behind the 1,454 publicly reported destructive ransomware events. In 2017, there were only three cataloged by RiskRecon. There were 42 active groups identified in 2023. That is a 14x increase in threat actor groups.

"From 2017 through 2023, 92 different criminal groups were behind the 1,454 publicly reported destructive ransomware events."

Destructive ransomware gangs by year



Destructive ransomware attacks by criminal group – top 20



So, what does settling in for the long haul in the battle against ransomware mean? 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 I.T. and cybersecurity well. Ensuring your suppliers are doing the basics well is now more important than ever.

"According to Coveware's Q4 2023 ransomware report, 24% of ransomware attacks start with phishing."

The U.S. Cybersecurity and Infrastructure Security Agency reemphasized doing the basics well in their ransomware advisory.[2] Keep software up to date, don't expose RDP to the internet, require multi-factor authentication for remote access, operate an email phishing defense program, and maintain robust backups of your mission-critical systems.

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, we call out a few key controls commonly cited in reputable sources and standards that you should consider adding to your supplier assessment criteria.

1. Operate an effective backup and restoration program.

   - Make regular backups of all data files necessary to restore business operations in the face of systems, applications, and data loss.
   - Periodically restore systems from backup to ensure that backups are sufficient to restore operations quickly.
   - Create offline backups 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 a ransomware-specific response playbook.

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

   According to Coveware's Q4 2023 ransomware report, 24% of ransomware attacks start with phishing.[3] 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.

[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

[3] https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

"15% of ransomware attacks started with exploiting vulnerable software in an internet-facing system."

4. Only expose authorized and hardened network services to the internet.

   Sharing the lead with phishing, 28% of ransomware attacks start by exploiting an internet-accessible RDP service. 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 required, explicitly authorized, and 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 that requires two-factor authentication should be used.

5. Keep software patches current.

   According to Coveware, in Q4 2023, 15% 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. Use services like RiskRecon to objectively verify and monitor your vendor performance to this requirement.

6. Prevent malware from being delivered and spreading to devices.

   - Filter malicious emails prior to 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 are installed on the host system. However, they don't provide 100% protection.

"It is essential to have robust network and endpoint activity and threat monitoring and blocking."

Two additional controls will greatly enhance the defensibility of systems.

- Remove administrator privileges from users and applications. This single action will prevent 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 preventative 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 U.K. National Cyber Security Centre https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
   - 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

"You can outsource your systems and services, but you can't outsource your risk."

No company can operate well without its suppliers reliably delivering goods and services. Ransomware threatens the operations of nearly every vendor in your supply chain. Fortunately, successfully managing the risk of ransomware requires doing the basics of I.T. and cybersecurity really 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.

Factor in the criticality of your suppliers, prioritize assessing the poor performers, and determine if they will 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

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.