riskrecon

mastercard

The Cybersecurity Hygiene of Ransomware Victims

Analysis of the cybersecurity state of ransomware victims at time of detonation

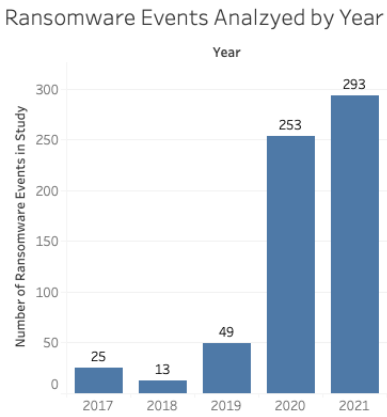
riskrecon.com

sales@riskrecon.com

Introduction

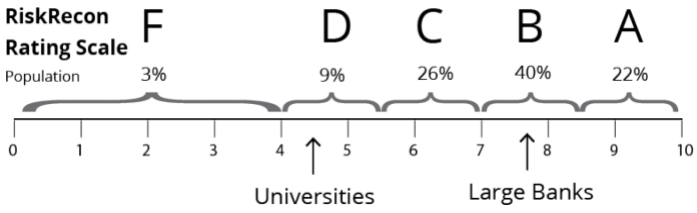
Any company operating a modern information technology environment can fall victim to system-encrypting ransomware. But not every company has fallen victim. Do companies that experience an operations-impacting ransomware event have poor cybersecurity hygiene? Or is the quality of cybersecurity hygiene not a factor in frequency of ransomware events?

To answer these questions, RiskRecon analyzed the cybersecurity hygiene on the day of ransomware detonation for 622 organizations spanning 633 ransomware events occurring between 2017 and 2021. The study population consists of publicly reported ransomware events in which the victim's systems were encrypted. The graph to the right shows the count of ransomware events included in this study by year. We did our best to include all events publicly reported in 2020 and 2021.



To understand the influence of cybersecurity hygiene on ransomware event frequency, RiskRecon compared the cybersecurity hygiene of victim companies against the hygiene of a general population of approximately 100,000 companies.

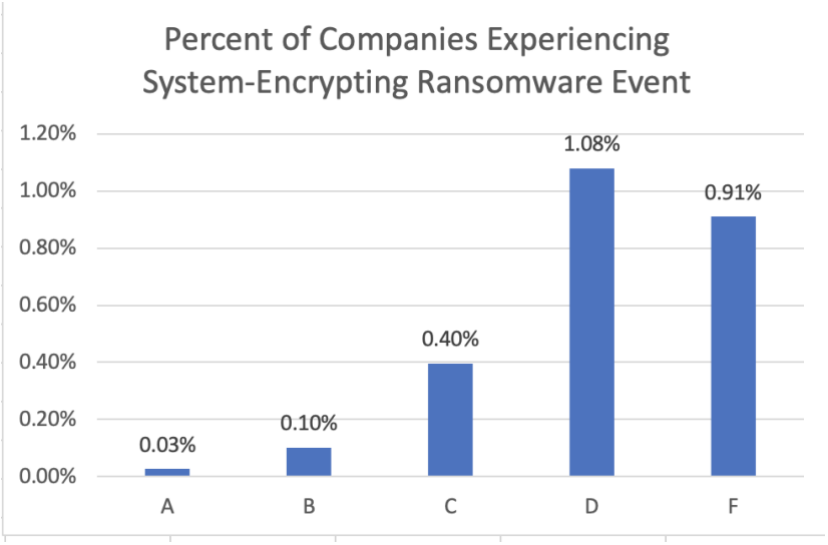
To conduct this analysis, RiskRecon leveraged its cybersecurity ratings and platform to assess the quality of the cybersecurity hygiene of each company at the time of ransomware detonation. As a leading cybersecurity ratings platform, RiskRecon continuously monitors the cybersecurity quality of millions of companies using passive assessment techniques. RiskRecon's assessments 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 this study was based is shown below.



The Correlation

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. For example, ransomware victims have an average of 11 material software vulnerabilities in their internet facing systems, in comparison with only one issue in the general population. That is 11 times higher! Looking at network services that criminals commonly exploit, ransomware victims expose 3.3 times more unsafe network services to the internet than the general population.

The table below contains a comparison of the cybersecurity conditions of victim companies at the time of ransomware detonation relative to the general population of approximately 100,000 companies.

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%	3x 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

In comparison with the general population, the cybersecurity hygiene of victims of ransomware is very unhealthy, on average.

Conclusion

The data clearly shows that good cybersecurity hygiene matters. On average, companies experiencing system-encrypting ransomware events that are significant enough to be newsworthy have significantly worse cybersecurity hygiene than the general population. Based on RiskRecon's analysis of their internet-facing systems they 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.

While the cybersecurity hygiene issues RiskRecon observes through its passive analytics of Internet facing systems and accessible signals may not be the exact vectors the criminals exploited to compromise each victim organization, their presence is a strong indicator that these organizations, on average, do not have robust cybersecurity risk management programs.

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.