riskrecon

mastercard

Change in Cybersecurity Hygiene One Year After Ransomware

An analysis of how the cybersecurity hygiene of companies changes one year after a ransomware event

riskrecon.com

sales@riskrecon.com

Introduction

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.

On the surface, this seems that it would be true, particularly for companies experiencing a system-encrypting ransomware event. What could be more motivating to get your cybersecurity house in order than a ransomware event that disrupts your ability to operate? So, do companies who have experienced a destructive ransomware event observably improve their cybersecurity hygiene? What about different industries? Do some industries respond to ransomware events better than others? In this study we answer that question by comparing the cybersecurity state of 181 victim companies on the day ransomware was detonated in their environment with their cybersecurity state one year later.

The Study

The study population consists of 181 companies whose ransomware event was publicly reported and resulted in disruption of operations due to system encryption. The population is also limited to those companies for which at least one year has passed since the ransomware event.

To measure how companies change their cybersecurity practices following a ransomware event, RiskRecon leveraged its cybersecurity ratings and platform to assess the cybersecurity hygiene of each company at the time of ransomware detonation and one year later. As a leading cybersecurity ratings platform, RiskRecon continuously monitors the cybersecurity quality of millions of companies using passive assessment techniques.

For this study, we focused our analysis on core cybersecurity hygiene practices that are central to defending against ransomware attacks and serve as a proxy for the overall quality of the cybersecurity program. These dimensions are strongly aligned with Coveware’s 2021 ransomware study as essential to defending against ransomware attacks, in which they found that 42% of ransomware attacks were initiated through compromising an unsafe network service, 42% through a phishing attack, and 14% through compromise of a software vulnerability.

Conditions Twelve Months Later – All Organizations

I am sorry to say it, but overall, companies don't show improvement in the cybersecurity hygiene of their internet presence one year after a system-encrypting ransomware event. At best, they take one step forward and one step back, showing improvement in software patching and degradation in restricting access to unsafe network services.

The table below details the mixed bag. On the positive side, one year after the breach, the number of victims with important software patching issues exposed to the internet decreases by 12% and, for those that still have material software vulnerabilities, they reduced their issue count by 15%. On the downside, the number of victim companies exposing commonly exploited network services increased by 50%. Remember that Coveware stat – percent of ransomware events start with a compromise of an unsafe network service?

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

Conditions Twelve Months Later – By Sector

For our analysis of cybersecurity hygiene at the industry level, we chose to look only at two dimensions – software patching and unsafe network services. Presenting all five security dimensions is just too much data for this summary paper. We have reserved detailed industry analyses for a separate piece.

By our research, the healthcare, education, and government sectors together accounted for 52% of all publicly-reported ransomware events occurring in the last few years. Given the pressure on the sectors, you would think their cybersecurity hygiene would markedly improve post-attack. Not so. The hygiene of victims in the government and healthcare sectors declined across both measures, increasing the amount of vulnerable software and unsafe network services exposed to the internet. While the education sector reduced their software

vulnerability exposure count by 21%, they increased the number of unsafe network services that criminals commonly compromise.

Professional services improved their software vulnerability management and network filtering practices. The software and transportation/logistics industries also improved their software patching practices while holding steady on controlling exposure of unsafe network services. Retail and finance were a mixed bag, improving in software patching while degrading in the other.

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

Industry	Security Domain	Day of Event Avg Issue Count	One Year Later Avg Issue Count	Change
Education	software patching issues	**18**	**14**	22% better
	unsafe network services	2	4	100% worse
Government	software patching issues	**`13**	**13**	no change
	unsafe network services	4	6	50% worse
Healthcare	software patching issues	**7**	**7**	no change
	unsafe network services	3	4	33% worse
Manufacturing	software patching issues	**20**	**24**	20% worse
	unsafe network services	15	19	26% worse
Professional Services	software patching issues	**9**	**7**	12% better
	unsafe network services	6	5	17% better
Software	software patching issues	**14**	**5**	64% better
	unsafe network services	3	3	no change
Transportation and Logistics	software patching issues	**7**	**6**	17% better
	unsafe network services	3	3	no change
Retail	software patching issues	**5**	**4**	25% better
	unsafe network services	2	5	150% worse
Finance and Insurance	software patching issues	**8**	**6**	42% better
	unsafe network services	8	10	25% worse

Conclusion

It seems that experiencing a major ransomware event, one significant enough to be newsworthy, would motivate an organization to markedly improve its cybersecurity posture. The evidence does not support that conclusion. At best, it is a mixed bag, with organizations improving their software vulnerability management discipline while still struggling to control the network services they expose to the internet.

It seems odd that this is the case. During our research, we noted that many companies were increasing their cybersecurity spending in response to the attacks. Yet the results of the reported increase in funding don't appear to materially improve their conditions. Perhaps it is true that good cybersecurity isn't something that you can just buy; it takes strong, consistent prioritization and support from the top that drives a change in the way the organization operates. That is hard.

Companion Paper

This paper is accompanied by another RiskRecon research paper titled "The Cybersecurity Hygiene of Ransomware Victims." In this paper, we reveal the cybersecurity conditions of ransomware victims at the time of detonation. We also benchmark their cybersecurity performance against that of the larger population.

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.