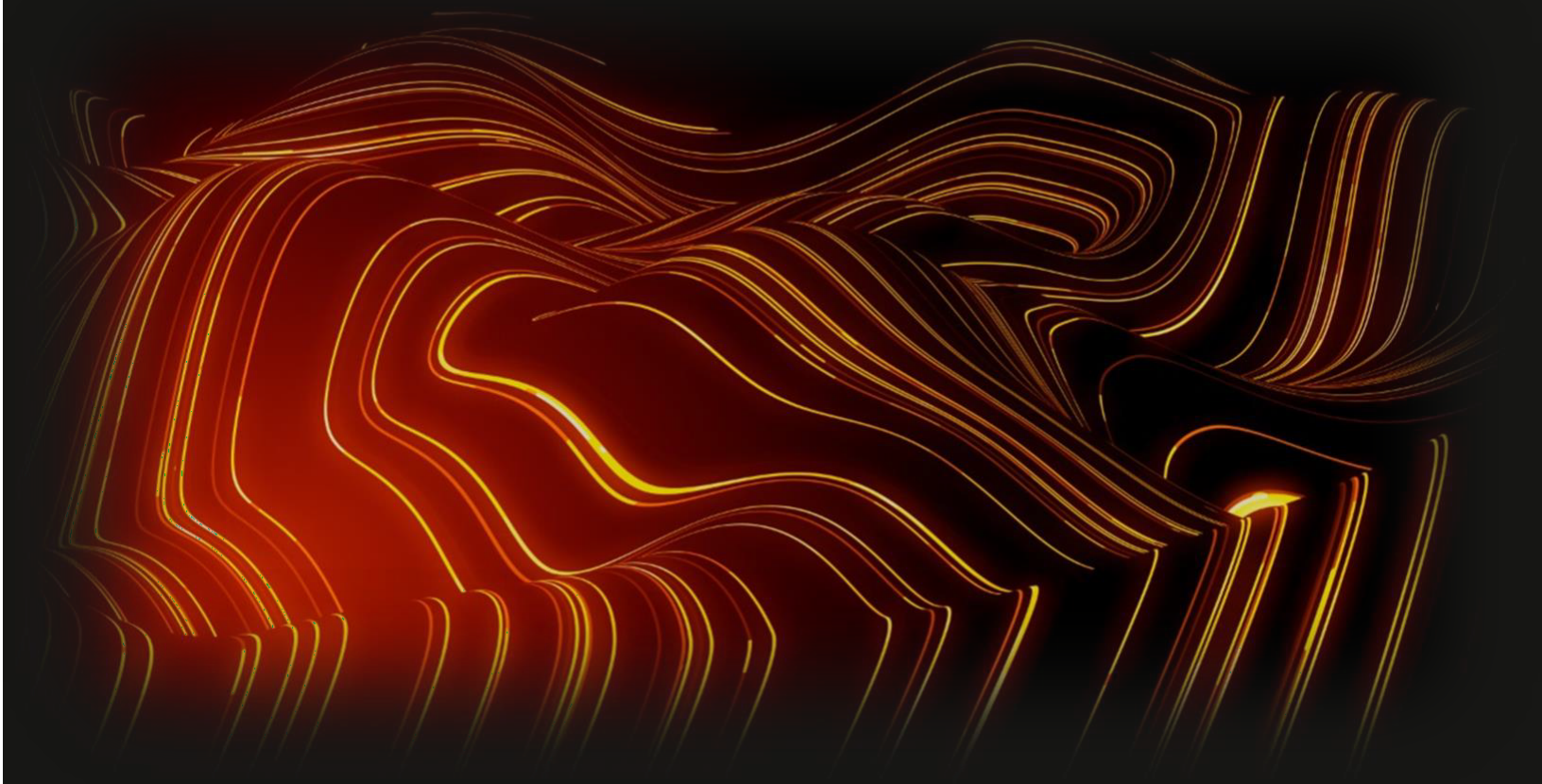
Risk Insights from 10 Years of Breach Event Monitoring of 196,000 Companies

THOUGHT LEADERSHIP PAPER

JULY 2025



Contents

Introduction

Welcome to the RiskRecon by Mastercard 10-year breach event study, spanning the years 2015 – 2024, and covering 196,000 closely monitored organizations. Our detailed analysis of these companies and the 20,421 breach events these organizations reported reveal many valuable insights that we are confident will be powerful inputs to your risk management program. Here are just a few interesting stats.

- In 2024, 1.3% of monitored companies publicly reported a breach event.
- Between 2015 and 2024, 8.1% of companies publicly reported at least one breach event.
- From 2015 to 2024 the number of publicly reported cybersecurity breach events increased nearly 450%, from 591 to 2,647.
- In the peak year of 2023, 1.8% of companies reported at least one breach event.
- Energy had the highest rate of breach events, with 65 breach events for every 100 energy companies monitored during the 10 years. The healthcare sector had the second highest rate, with 34 of every 100 organizations reporting a breach during the same period.
- Organizations with attack surfaces having greater than 5,000 internet-facing systems have a 20 times greater frequency of publicly reported breach events compared with the smallest companies, having 10 or fewer systems.
- 68% percent of breach events were publicly reported within 30 days of initial breach.
- 7% of breach events took more than 12 months to report after the date of the initial compromise.
- Insider actor breach events took nearly twice as long to discover, and report compared with external actor and vendor-centric breach events.
- External actors accounted for 57% of breach events. Internal actors accounted for 16% of events, and Partners accounted for 17%.
- The breach event frequency for companies with very clean cybersecurity hygiene ('A-rated' by RiskRecon) was 3.6 times lower than for companies with very poor cybersecurity hygiene (rated as 'D' or 'F' by RiskRecon).

The remaining pages of the report have many more insights, with loads of graphs and data visualizations. Whether you are charged with protecting your own enterprise infrastructure, managing third-party risk, or underwriting cyber insurance policies, we are confident you will find many valuable insights here that will help you better manage risk.

Breach event studies vary in the quantity of breach events due to uneven information research and what is counted as a breach event. This study only includes high confidence events, limited to those in which data was stolen, or systems were encrypted AND there was strong evidence of actual breach as evidenced by confirmation by the victim organization or public disclosure of the stolen data. This study does not include "incidents" in which there was an intrusion, but the incident was contained such that there was no harm to the organization or its data.

Regardless of the differences in studies, the breach event frequency trends, underlying actors and methods, and the cybersecurity conditions of breached organizations is very valuable.

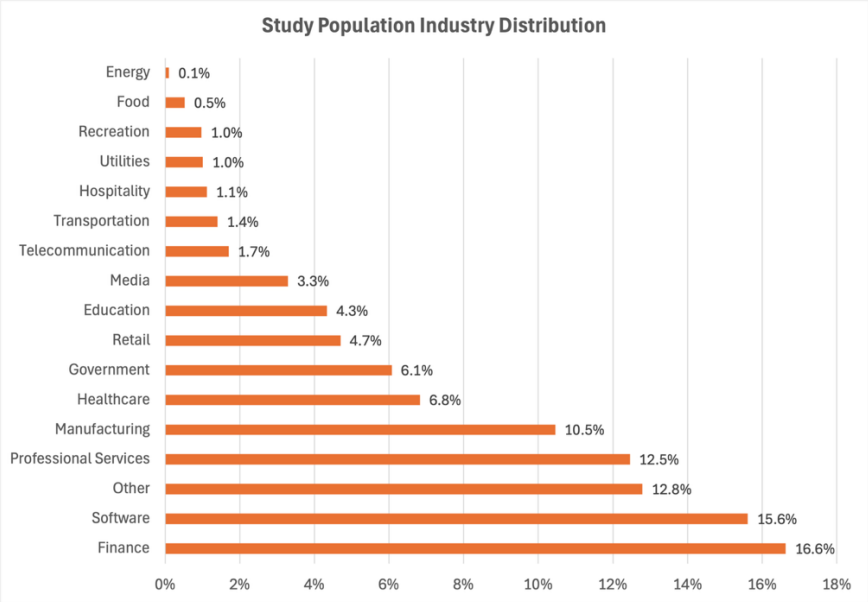
Methodology and Study Population

RiskRecon continuously monitors the cybersecurity hygiene of over five million organizations, spanning all industries and nearly all parts of the globe. For purposes of this study, we selected 196,000 companies for which RiskRecon maintains human-supervised, continuous cybersecurity assessments on behalf of its customers which have particularly high-risk relationships with these organizations. Beyond continuously analyzing the cybersecurity configurations of each company's internet-facing systems and related signal intelligence, RiskRecon analysts catalog breach events occurring within each company. Analysts source data loss events from channels such as public media, regulatory filings, and dark web monitoring.

For purposes of this study, breach events are limited to the 10 years spanning January 1, 2015, through December 31, 2024. From each of the breach disclosures, RiskRecon analysts recorded data such as the breach event date, the breach disclosure date, the primary actor, the reported compromise vector, and the number of records stolen. This data, combined with RiskRecon's cybersecurity ratings and assessment data, combine to reveal some very interesting insights.

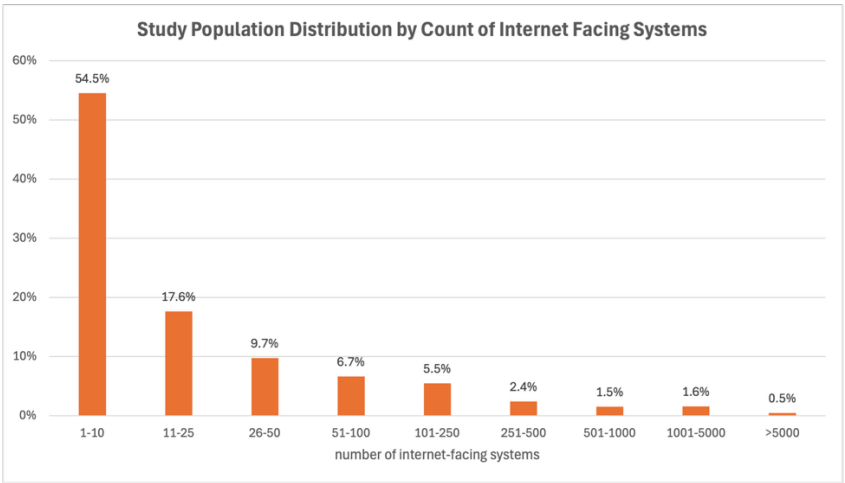
Industries

The study categorizes the organizations into 16 industries, with the remaining placed in the category of "other".



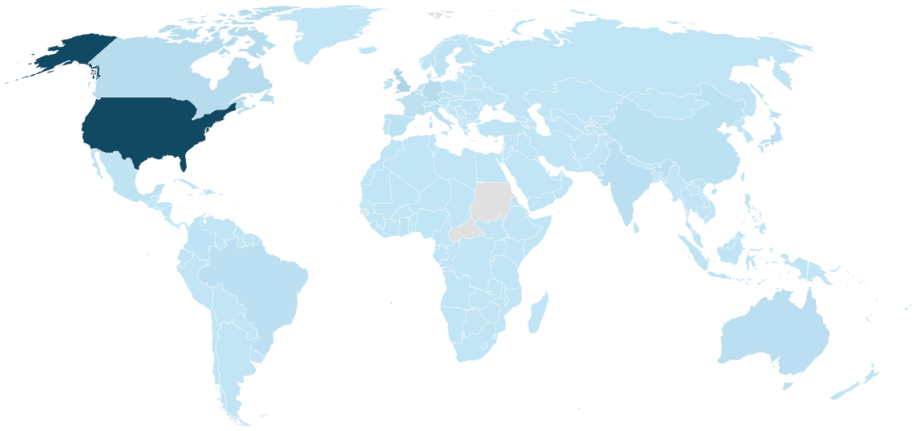
Size

The study population includes companies of all sizes of internet-facing infrastructure. Fifty-four percent of companies have 10 or fewer systems in their internet attack surface, while 2.1% have more than 1,000.



Geography

The study encompasses companies with primary centers of operation in 245 countries and territories. Most of the organizations are based in the U.S., accounting for 54% of the population. The United Kingdom accounts for 7%, Germany for 4%, and Canada for 3%. Australia, India, China, and Brazil, France, Japan, and Spain each account for between 1% and 2%.

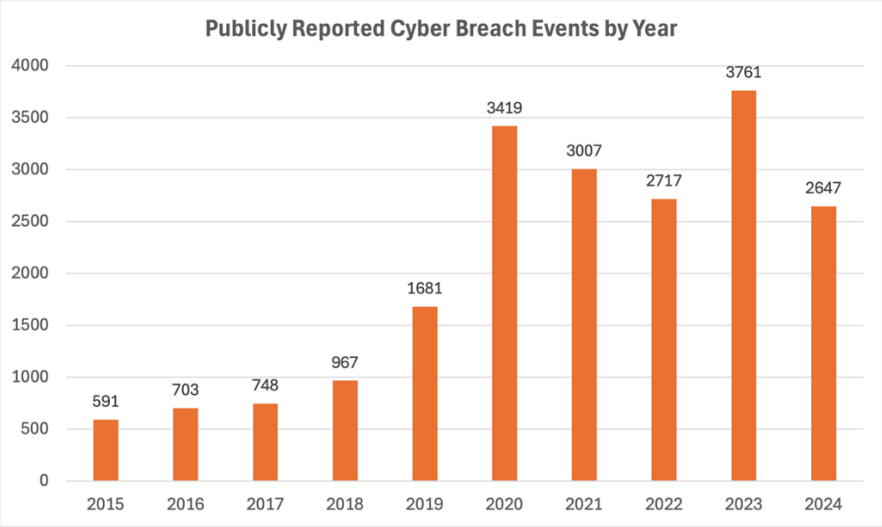


Disclaimer

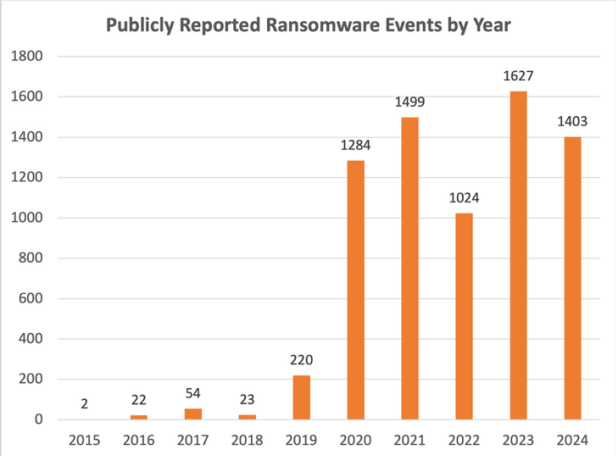
Public breach event notifications are biased and unevenly reported over time. Not all companies publicly report all breach events; it varies based on factors such as geography, industry, the quality of governance, and even the ability to detect a breach at all. Even for countries that now have strict public breach reporting requirements, such as the United States and Europe, the reporting requirements were not as strict in 2015 as they were in 2024. So, we do our best with the data we have.

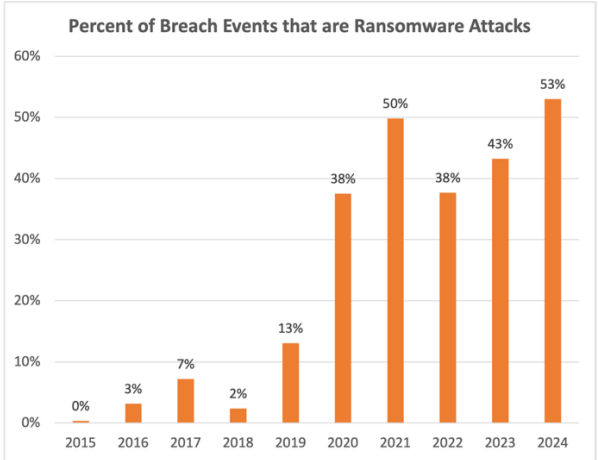
Top-Level View

Between 2015 and 2024, RiskRecon analysts identified 20,241 publicly reported breach events within the population of 196,000 organizations. During this time breach events grew at a compound annual growth rate of 16%. It would have been much higher if we ended the study in 2023 when we cataloged a stunning 3,761 breach events. Fortunately, 2024 closed out at a five year low at 2,647 events, 30% lower than 2023.

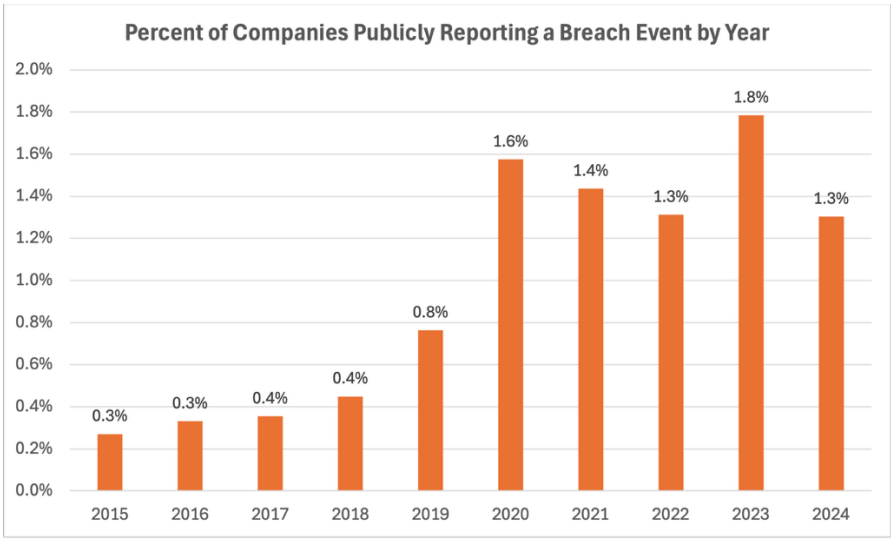


Ransomware has taken the center stage of breach events, growing from just two events in RiskRecon's catalog in 2015 to 1,403 in 2024 – 53% of all breach events that year.

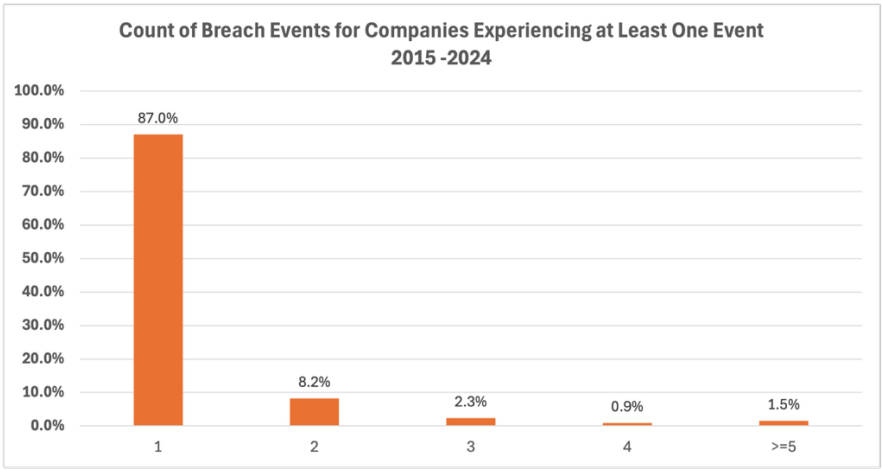




Of the 196,000 organizations, 8.1% of the companies (15,896) publicly reported at least one breach event between 2015 and 2024 – just over 1 in 12. In 2024, 1.3% of all companies reported being breached, down from 1.8% in 2023.



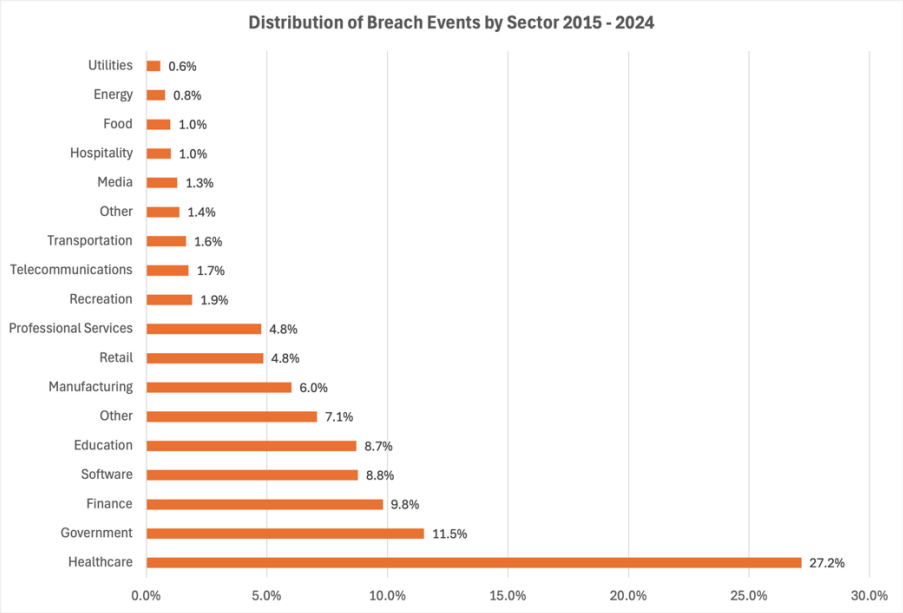
Of the 8.1% of organizations reporting a breach from 2015 - 2024, 87% reported just one event, while 1.5% reported five or more. Of the top 10 organizations disclosing the highest number of breach events, four were national governments and two were US state governments. The remaining spanned retail pharmacy, healthcare, social media, and software.



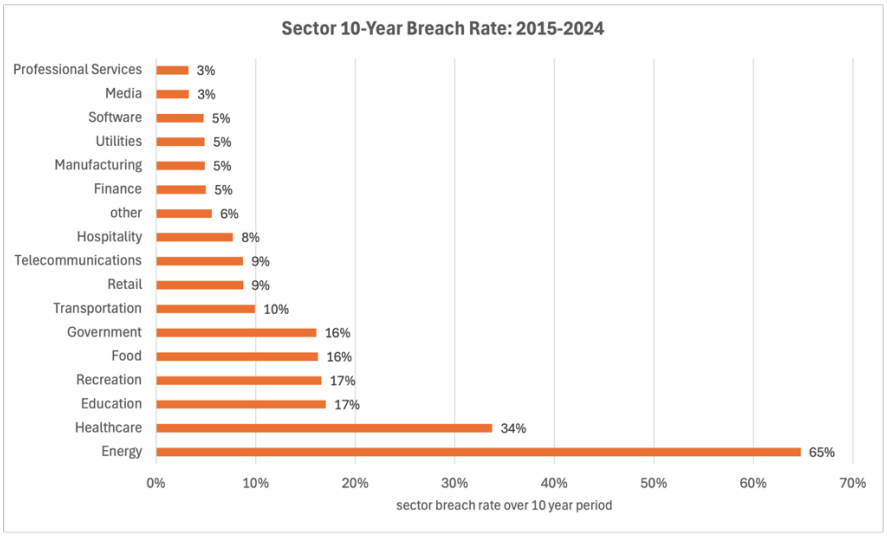
RiskRecon Risk Management Insights: In the peak year of 2023, 1.8% of companies publicly reported a breach event. For those managing third-party risk, this serves as a good minimum baseline for vendor breach volume. At that rate, a portfolio of 500 vendors, which isn't unusual, would have to manage the impact of nine publicly reported vendor breach events per year.

Industry View

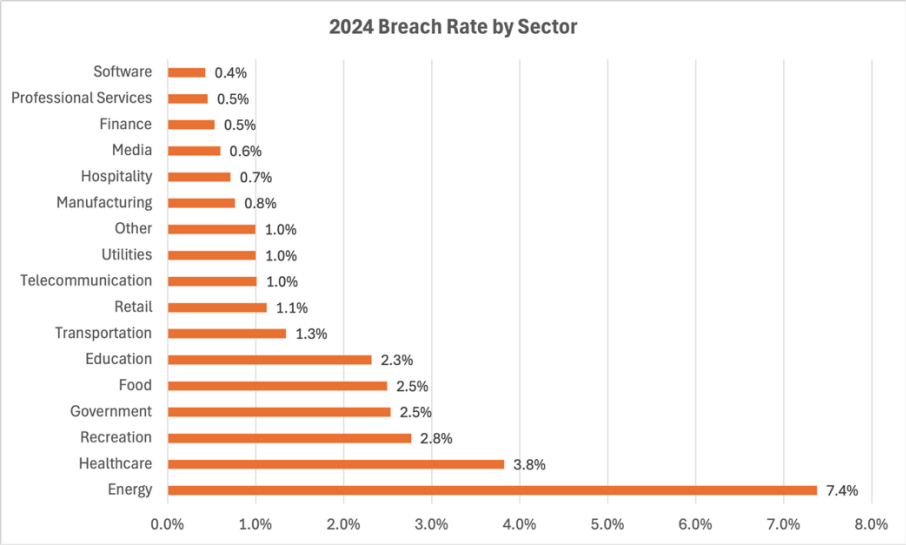
Looking at the sheer count of breach events from 2015 through 2024, the healthcare sector had the highest volume, accounting for 27.2% of all breach events (5,500 events). The government sector followed distantly at 11.5% of all events and finance at 9.8%.



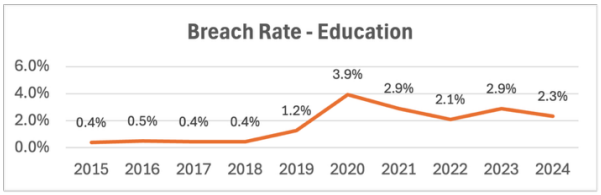
It is a different story when you look at the rate of breach events by sector across the same period. The energy sector had the highest breach rate with 65 reported events for every 100 monitored entities. Healthcare came in at 34 events for every 100 organizations, double the rate of recreation, education, food, and government.



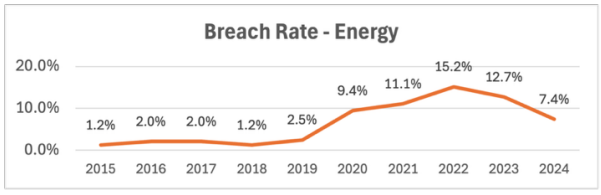
Secor breach event rates for the year 2024, energy had the highest at 7.4 breach events for every 100 enterprises. Healthcare closed 2024 with 3.8 breach events for every 100 providers.



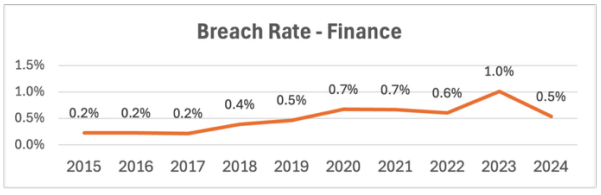
Looking at annual breach trends at the sector level, 14 of the 17 industries closed out 2024 with significantly lower breach rates than their highs. Only utilities reached a new high, increasing from 0.6% in 2023 to a 1% breach rate in which one of every 100 utility companies publicly reported being breached. Two sectors, media and other, tied their prior high marks.



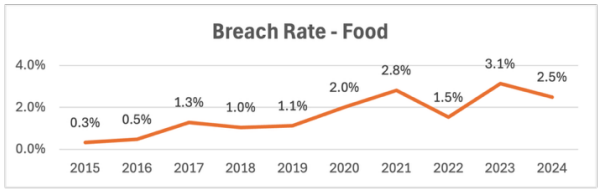
Education: Down 41% from 2020 high of 3.9%.



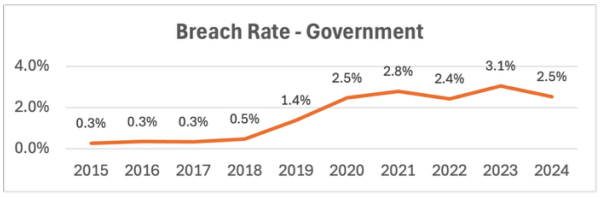
Energy: Down 51% from 2022 high of 15.2%.



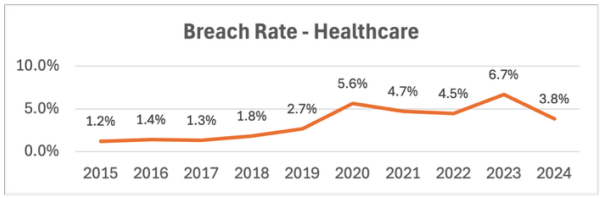
Finance: Down 50% from 2023 high of 1%.



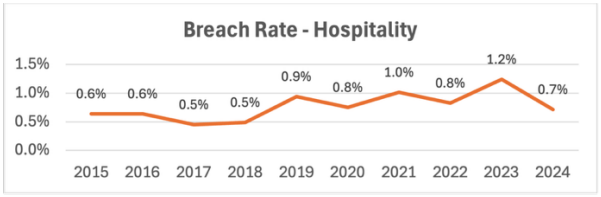
Food: Down 20% from 2023 high of 3.1%.



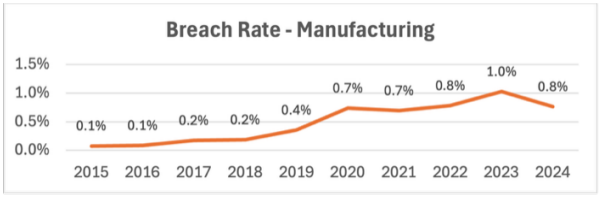
Government: Down 20% from 2023 high of 3.1%.



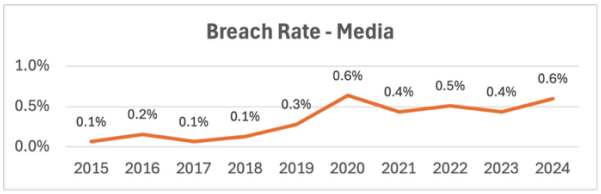
Healthcare: Down 43% from 2023 high of 6.7%.



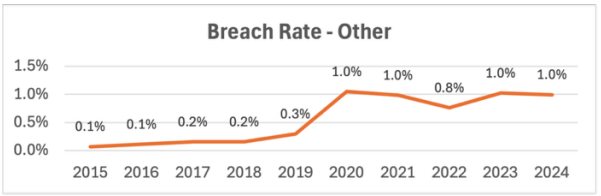
Hospitality: Down 42% from 2023 high of 1.2%.



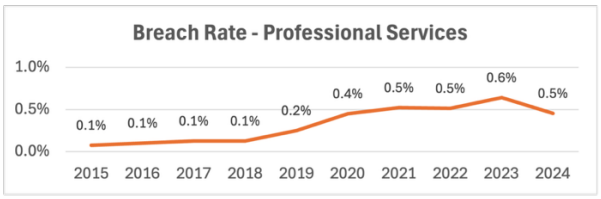
Manufacturing: Down 20% from 2023 high of 1.0%.



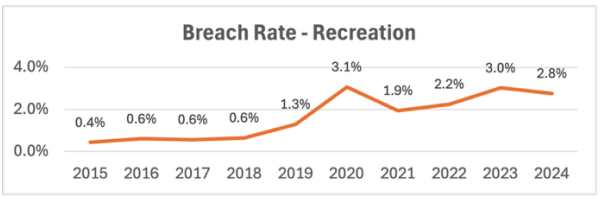
Media: Tied with 2020 high of 0.6%.



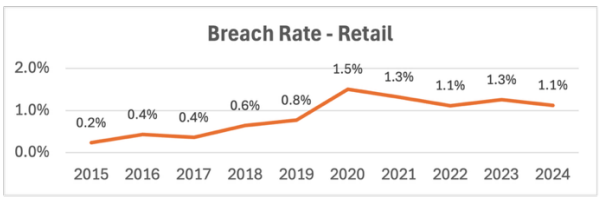
Other: Tied with 2020 and 2023 high of 1.0%.



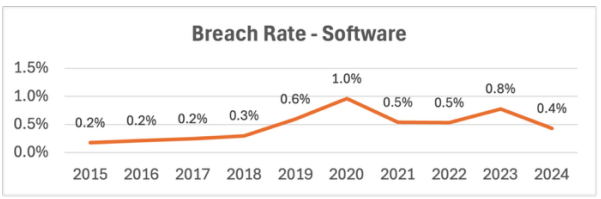
Professional Services: Down 20% from 2023 high of 0.6%.



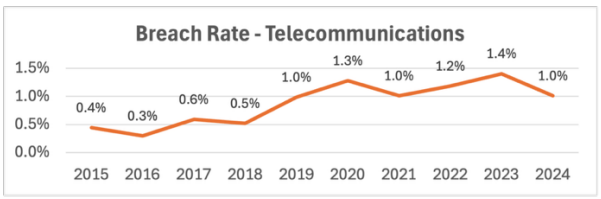
Recreation: Down 10% from 2020 high of 3.1%.



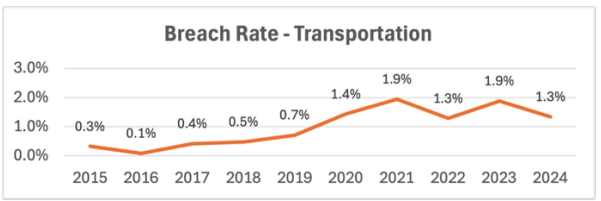
Retail: Down 27% from 2020 high of 1.5%.



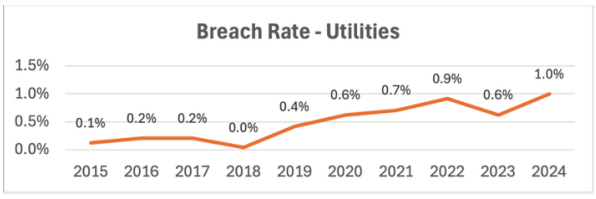
Software: Down 60% from 2020 high of 1.0%.



Telecommunications: Down 29% from 2023 high of 1.4%.



Transportation: Down 32% from 2023 high of 1.9%.



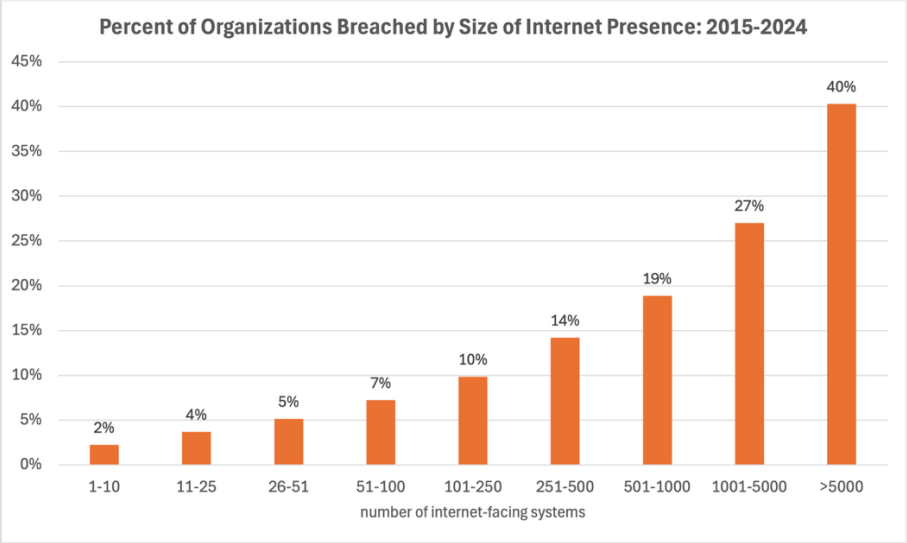
Utilities: At an all-time high in 2024, up 67% over 2023.

RiskRecon Risk Management Insights: Every sector is under significant threat pressure. While breach rates for most sectors are down from their highs, they remain at a material level. Breach rates for nine of the sectors increased over 6-fold in 10 years.

Risk managers would be wise to update their industry-specific cybersecurity risk models. Those using old data will dramatically underestimate breach event frequencies.

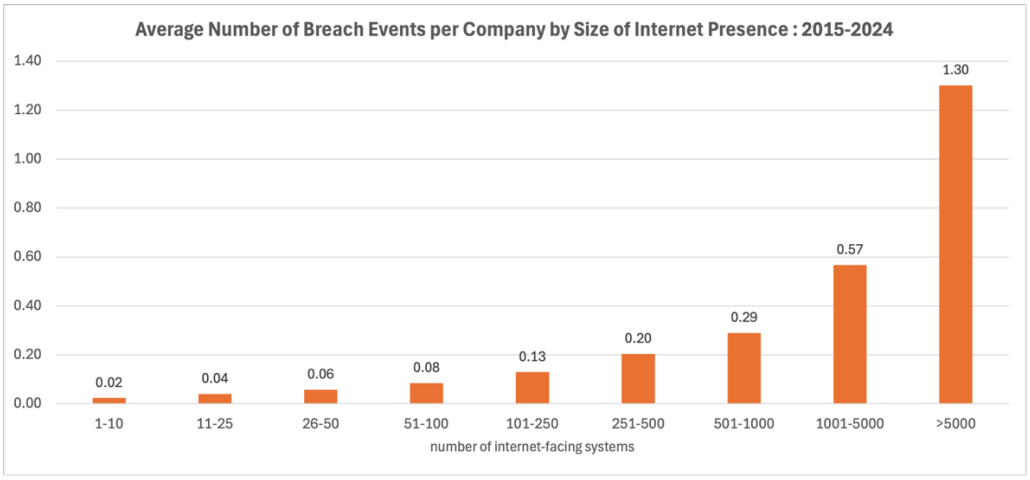
Company Size View

One of the best predictors of the publicly reported breach event frequency may be the size of the organization's internet attack surface – the number of systems the company operates on the internet. The larger an organization's internet presence, the higher the frequency of breach events. Forty percent of companies with greater than 5,000 internet-facing systems publicly reported at least one breach event from 2015-2024. In comparison only two percent of companies with 10 or fewer systems publicly reported a breach.



Organizations with >5,000 internet facing systems had **20x higher** frequency of breach events than those with 10 or less.

Looking at the breach rate for companies of different sizes, those with the largest attack surfaces publicly reported an average of 1.3 breach events from 2015 to 2024. While only 40% of the largest companies reported being breached, many of them reported multiple breach events.



The net of it is that companies with the largest attack surfaces publicly report breach events 20X more frequently than the smallest organizations, so they are going to drive a lot of third-party incident response. However, that doesn't mean larger organizations are less competent; they are just having to protect more infrastructure, more processes, and more data.

RiskRecon Risk Management Insights: If you are managing third-party risk, you would be wise to factor the size of the organization's attack surface into your inherent risk model. The larger the attack surface, the higher the breach event frequency. Companies with >5,000 systems in their attack surface have a 20x higher breach event frequency!

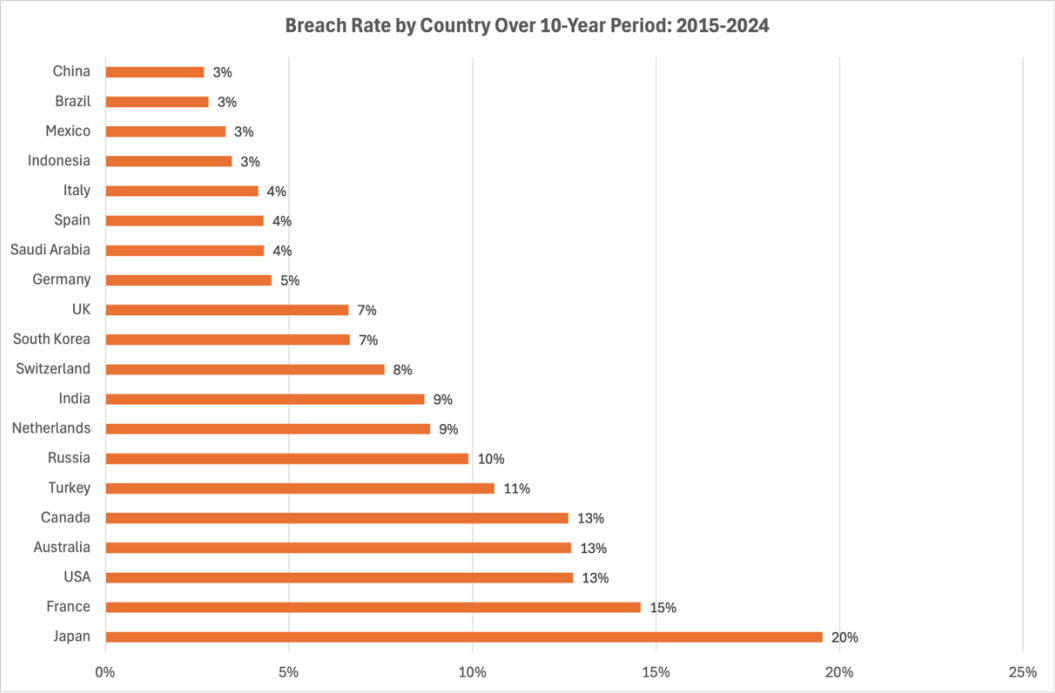
Your team will be assessing the impact of a lot of third-party breach events for those larger companies. It may be the case that the smaller companies aren't reporting breach events as well as the larger ones, but we won't know until someone reports it.

Geographic View

Across the 245 countries and territories that RiskRecon monitors cybersecurity conditions, RiskRecon cataloged breach events in 178 of the regions. While the bulk of the attacks follow the level of economic activity, some did reach remote areas such as Vanuatu, North Macedonia, and Nauru. Even Vatican City was hit. In the case of Vanuatu, the October 2022 attack shutdown government systems for over a month, forcing agency personnel to resort to typewriters, pen and paper, and Gmail to continue operations.

Country-Level Breach Rates Across 10 Years

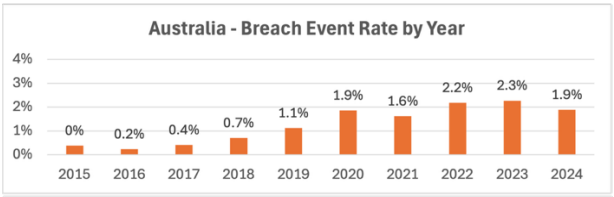
Looking at the top 20 countries by GDP, Japan had the highest reported rates where there were 20 breach events for every 100 monitored organizations in the period from 2015 - 2024. France took the next spot with 15 for every 100. The USA, Canada, and Australia both came in at 13 for every 100. Taking up the low end of the breach rates, China, Brazil, Mexico, and Indonesia all came in at around three breach events for every 100 organizations.

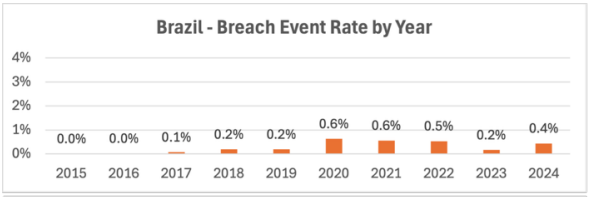


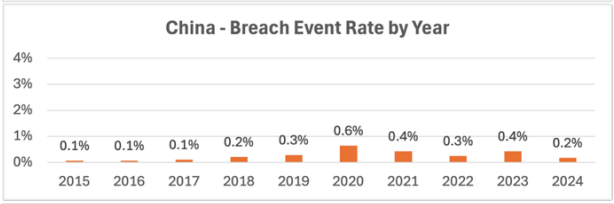
Analysis of geographic-specific breach events is difficult. Regional factors like cybersecurity regulations, breach reporting requirements, cybersecurity capability, and even freedom of the press strongly influence breach event reporting.

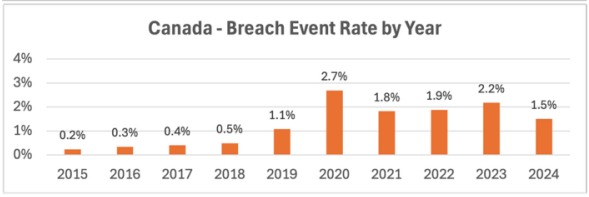
Country-Level Breach Rates by Year

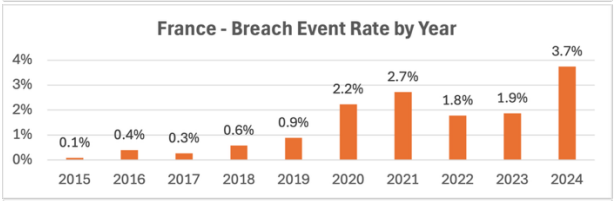
Examining country breach rates by year, in 2022 Russia recorded the highest single year breach rate with 4.1 of every 100 monitored organizations breached. In 2024 France came in with a high of 3.7 breaches for every 100 organizations. Fortunately, the overall trends improved in 2024 with 14 of the 20 countries coming in with rates lower than 2020 – five years ago.

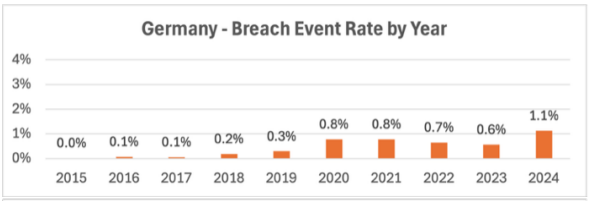


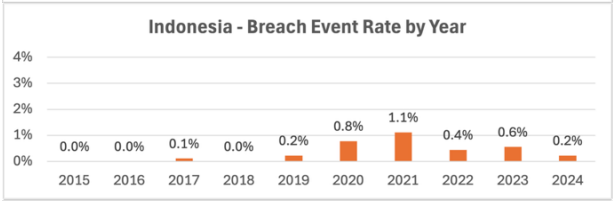


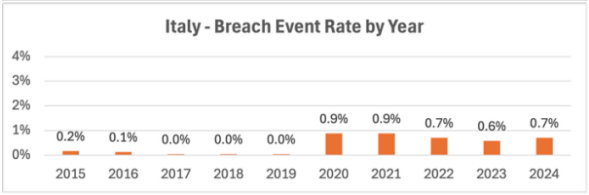


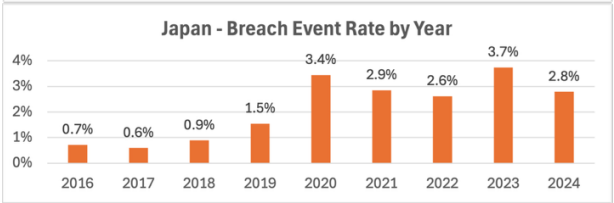


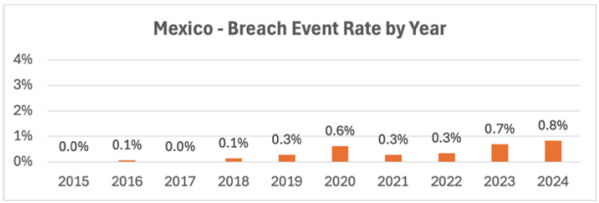


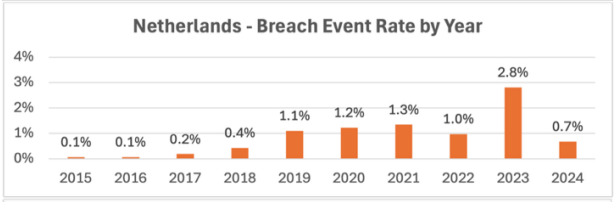


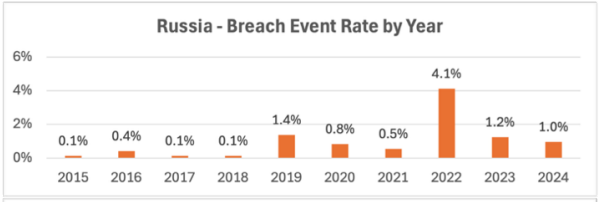


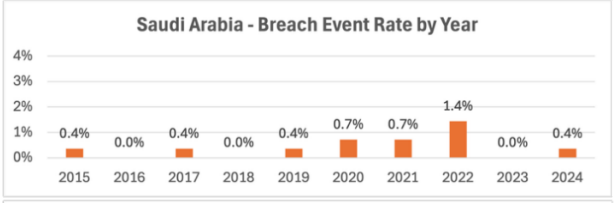


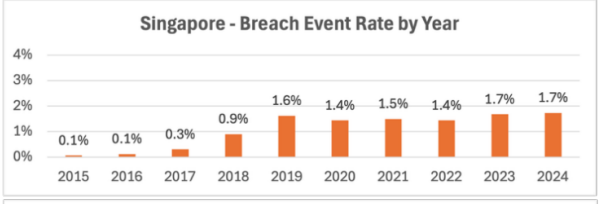


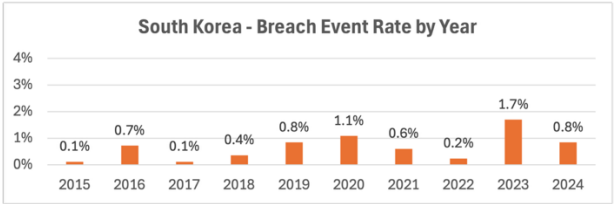


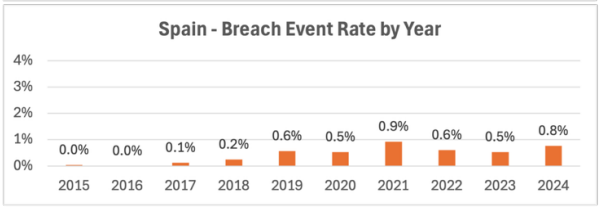


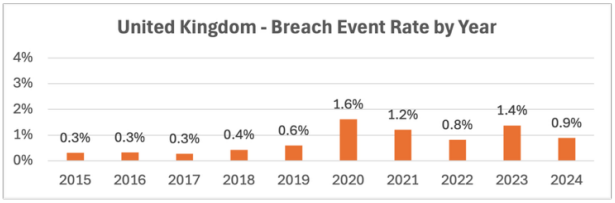


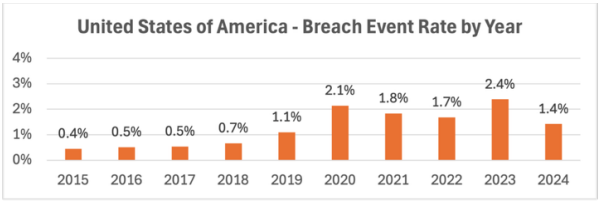






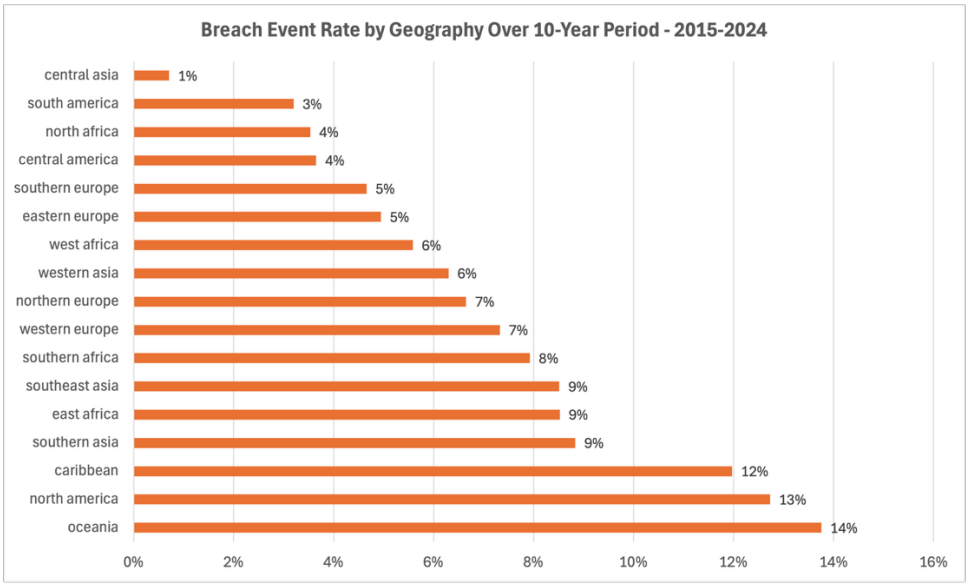






Region-Level Breach Rates Across 10 Years

Zooming out to macro geographic regions, about 3% of monitored companies in South America and 4% in North Africa and Central America publicly reported a breach event between 2015 and 2024. In comparison, 13% of organizations in North America reported a breach during the same 10-year span.



One of the surprises in the data is the very high breach rates in tech-savvy, highly regulated areas relative to less technology sophisticated and regulatory intensive regions. North America, Oceania, and Western Europd all come in 10-year breach rates of 7% or more over while regions such as South America, North Africa, and Central America are at 4% or less. How should one think about this? The following are worth considering:

- Many countries are underreporting or are not detecting breach events. Is it a good idea to outsource sensitive systems and services to regions that don't have strong cybersecurity and public breach reporting regulations? Regulations are a strong driver of cybersecurity investment. And public breach reporting rules put some accountability for performance on operators.
- Regions with strong breach event reporting regulations, such as Western and Northern Europe, North America, and Australia, generally have higher publicly reported rates of breach events. Is this because they are getting targeted more often? Or are they just better at detecting and reporting? It is likely quite a bit of both.
- The breach event rates of the regions with robust public breach reporting requirements likely are the baseline expected breach rate. Within a given year, we should expect to see 1% - 3% annual breach rate. Anything below 1% may indicate that events are not being reported.

RiskRecon Risk Management Insights: In evaluating vendors and their operational geographies, think seriously about the strength of the cybersecurity regulations and public breach event reporting requirements of the region. Regulations enforced, over time, build a baseline of competency and discipline.

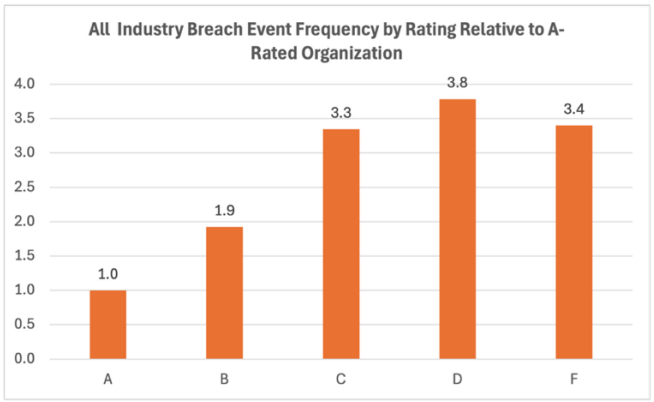
Cybersecurity Hygiene

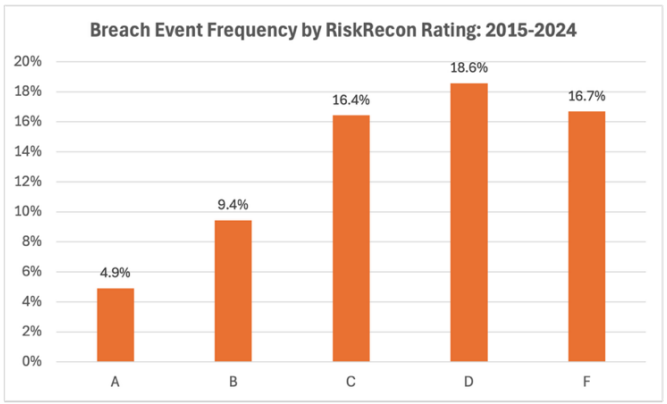
Do companies with good cybersecurity hygiene have lower rates of breach events? We answered this question by correlating the RiskRecon cybersecurity ratings and assessment information of each company with the breach event data. The RiskRecon cybersecurity ratings and assessment platform continuously monitors the cybersecurity hygiene of millions of companies, analyzing areas such as software patching, network filtering, and application security.

Organizations rated by RiskRecon as having very poor cybersecurity hygiene in their internet surface (a 'D' or 'F' RiskRecon rating) experienced a combined 3.6x higher frequency of breach events compared to A rated organizations, which RiskRecon observes as having very clean hygiene.

Organizations whose cybersecurity hygiene was rated as 'D' or 'F' by RiskRecon had a **3.6x higher** frequency of breach events compared with those earning an 'A' rating.

As a group, 51.7% percent of C, D and F rated companies have had a breach event since 2015. In comparison, only 4.9% of A rated companies and 9.4% of B rated companies have publicly reported a breach. In terms of the frequency of breach events, over 10 years A-rated organizations had 4.9 events for every 100 organizations, whereas F-rated organizations had 16.7 for every 100 organizations.





The cybersecurity conditions underlying the RiskRecon rating reveal just how poor the cybersecurity hygiene is of companies, on average, at the time of the breach event. In comparison with the larger US healthcare population, those that experience a breach event, on average, have:

- Fourteen times more high and critical severity issues in their internet facing systems.
- Eight times more unsafe network services exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.

- Nine times higher frequency of application security issues such as not implementing encryption in systems that collect sensitive data and application platform administration interfaces exposed to the internet with single-factor authentication.
- Twelve times higher frequency of encryption configuration issues in high value systems that collect and transmit sensitive data.

Table: Comparison of the count of security issues in internet-facing systems surrounding date of breach against the count of security issues of the general population.

	Average Issue Count		
	Breached Company	**General Population**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	11.7	0.8	14.6x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	18.9	2.3	8.2x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	50.7	4.3	11.8x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	20.2	2.3	8.8x higher

Ignoring issue counts and just looking at the percent of companies with one or more significant issues across the RiskRecon cybersecurity domains, the material breach event victim group again stands out as having very poor hygiene in comparison to the general population.

- 2.8 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.
- 1.5 times more organizations with at least one application security issue such as not implementing encryption in systems that collect sensitive data and application platform administration interfaces exposed to the internet with single-factor authentication.
- 1.3 times more companies with at least one web application that transmits sensitive data that has HTTP encryption issues such as expired certificates, weak encryption algorithms, or invalid certificate subjects.

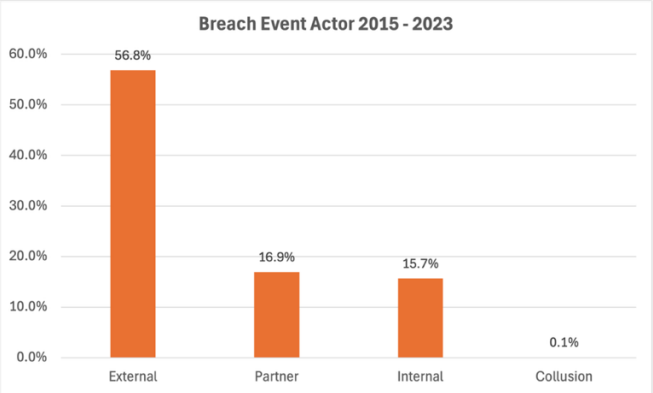
	Percent with at Least one Issue		
	Victim at Time of Breach	All Organizations	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	42%	15%	2.8x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	39%	19%	2.1x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	35%	28%	1.3x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	51%	34%	1.5x higher

Companies with good hygiene get breached, but as a group they are breached much less frequently. They are simply more difficult to compromise, and they are more likely to have detective and response controls that detect the compromise before it escalates to a publicly reportable breach event.

RiskRecon Risk Management Insights: Do business with companies that have good cybersecurity hygiene. The data shows that those with good hygiene have a 3.6 times lower rate of publicly reported breach events relative to companies with poor hygiene. RiskRecon cybersecurity ratings can help you quickly sort those with good hygiene from those with poor hygiene.

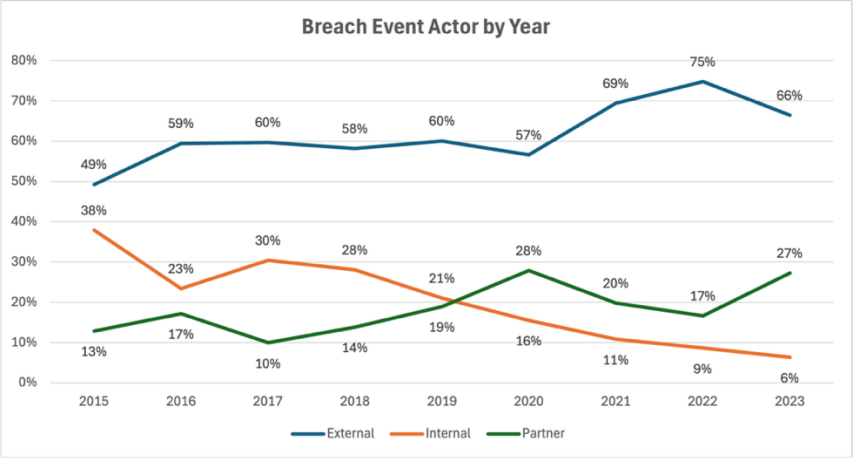
Breach Actors

For 86% of the breach events the general threat actor was disclosed in the public notifications. From 2015 through 2023, 56.8% of breach events were attributed to external threat actors, followed by 16.9% attributed to partners, and 15.7% to internal actors[1]. A tiny fraction of disclosures, 0.1%, revealed that insider collusion with an external agent was at play in executing the attack.



Looking at the breach event actor distribution by year, back in 2015 breach events caused by external actors compromising an organization was close to that of internal actors. Since then, they have gone in opposite directions, with external now accounting for 66% of breach events. No doubt, the ability to monetize breaches through crypto-based ransom demands is one of the drivers behind this growth.

Likely driven by the massive outsourcing of systems and services, the percentage of breach events attributed to partners has outstripped that of insiders since 2019 and the gap is growing, with the latest year attributing 27% of all breach events to partners compared with 6% to insiders.



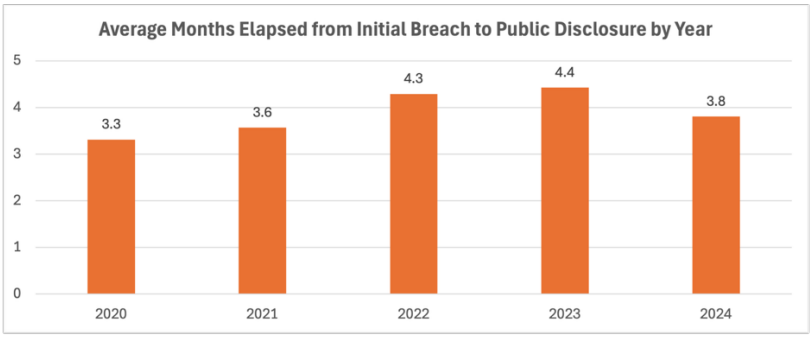
Relative to other actors, insider-driven events were subdued, reaching a low in 2023 of 6% of all events. This is a decrease from the high-water mark in 2015 when insiders were behind 38% of all events. Keep in mind, while insider activity decreased relative to the total events, insider breach events still increased by 40% over the period.

[1] Attribution of breach events to threat actor category is only provided from 2015 – 2023 because the 2024 data had not yet been compiled at the time of the publication of this study.

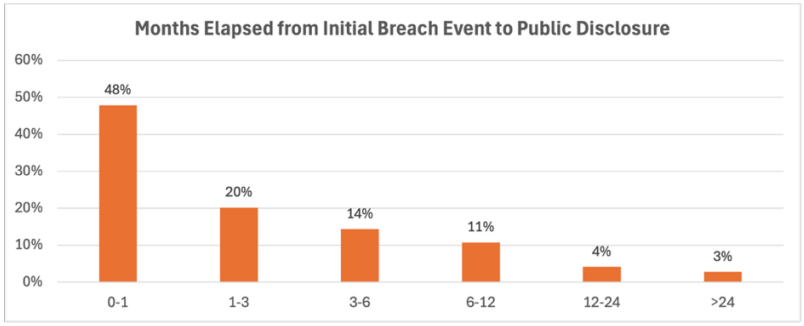
RiskRecon Risk Management Insights: Unfortunately, you can't take your eye off any threat actor – they are all active. The count of events was higher for every actor in 2023 was higher than in 2015. One thing stands out though – external actors are pressing hard against enterprises and their partners. It will take a serious improvement in defenses to successfully stand against them.

Time Elapsed from Breach to Public Disclosure

Looking at the annual data for the last five years, the time elapsed between initial breach and public disclosure has ranged from 3.3 months to 4.4 months, with 2024 coming in at 3.8 months.



Over the last ten years, 68% of breach events were publicly disclosed in less than three months from the date of initial breach. This seems reasonable given some days to detect the event, followed by weeks to investigate, and then work with legal and PR to formulate and submit the necessary filings and disclosures.



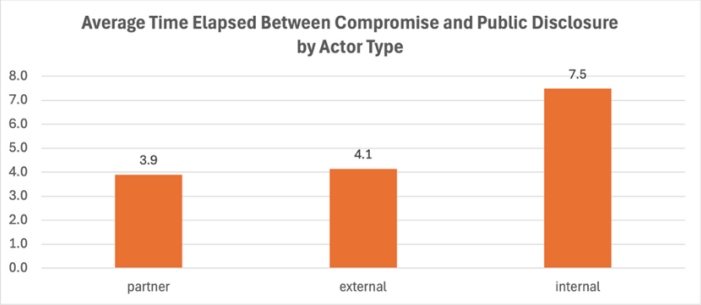
The events of particular interest are the 7% that take longer than twelve months to disclose. In most of these cases the systems were compromised long before detection. Here are some examples of delayed disclosure breach notices:

- "[COMPANY] identified an intrusion on December 24, 2018, when GandCrab ransomware was used to encrypt files on its network. The forensic investigation confirmed the attackers first gained access to its network on April 1, 2017."
- "It has been discovered that some of the data that [COMPANY] entrusts with [OTHER COMPANY] for management has been made public due to incorrect settings in the cloud environment…Period during which it was accessible from outside: November 2013 – April 2023."
- "The investigation ultimately determined that a small subset of emails may have been accessible to

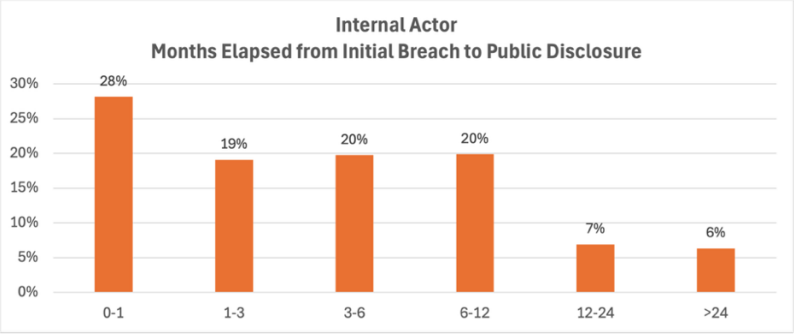
an unknown individual between February 7, 2017, and August 28, 2023."

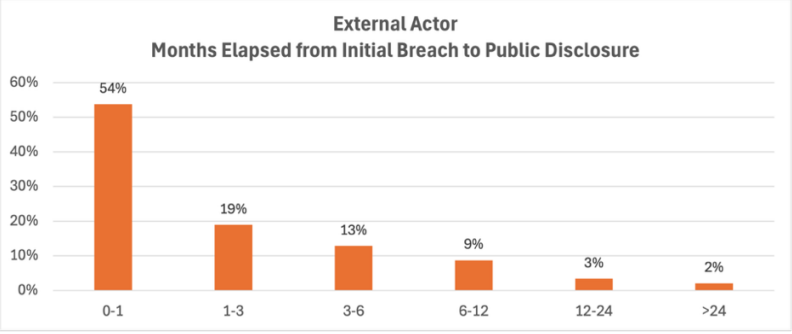
- "From at least 2015 until 2017, he stole software from [COMPANY], along with sensitive government data bases containing personal identifying information of [COMPANY] employees..."
- "Japanese game developer [COMPANY] has proven that a simple Google Drive configuration mistake can result in the potential but unlikely exposure of sensitive information for nearly one million people over a period of six years and eight months."
- "After thorough investigation, it was determined that the employee improperly accessed certain patient information between October 2009 and February 2019."

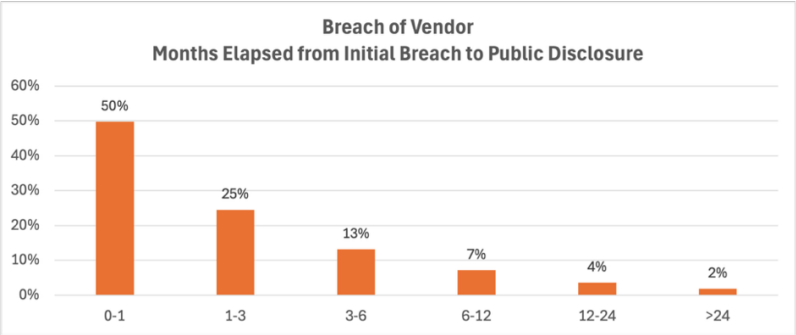
Disclosure of breach events executed by an insider took the longest to disclose, averaging 7.5 months, likely reflecting the difficulty of discovering malicious insider activity. External actor breach events took 4.1 months to disclose, and partners took 3.9 months. Insider breach events likely take the longest to detect because they commonly involve abuse of authorized privileges and errors that can be difficult to discover.



Comparing insider breaches against the other actors further, only 28% of insider events were reported within one month of the initial breach. In comparison, 54% of external actor events and 50% of partner events were reported within one month.

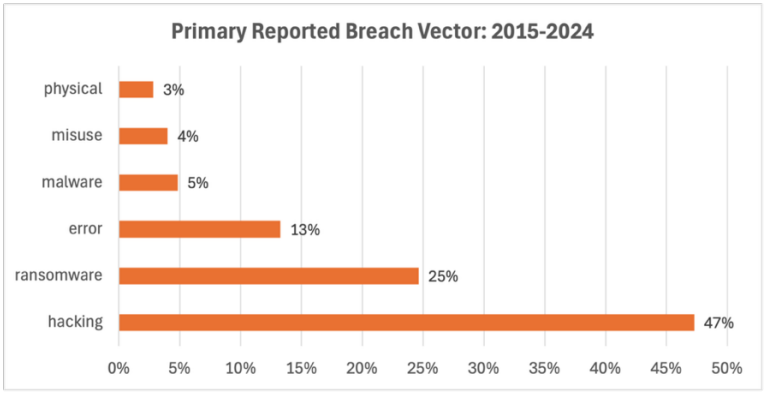






Breach Vectors

The primary compromise vector was publicly reported for 89% of breach events, though often in generic terms. Hacking was the top vector referenced in public notifications, representing 47% of all breach events. Ransomware was cited in 25% of the cases. Insider errors were pointed to for 13% of breach events and insider privilege abuse for 3%. Malware was referenced in only 5% of cases but is certainly under reported as it is likely behind reports that cited ransomware and hacking. Social engineering was cited in only 3% of breach notifications, but this is very likely vastly understated as a large percentage of malware infections and credential thefts occur through phishing.



The breach vectors are defined as follows:

- **Hacking** – Hacking is the most generic category cited in breach disclosures, being a catch-all for remote system compromise. It is likely that public disclosures referenced hacking generically, rather than citing more specific vectors such as malware.
- **Malware** – Malware includes all forms of malicious software deployed to endpoints and servers.
- **Ransomware** – The ransomware category is for those events in which reports specifically stated that the event was a ransomware attack. Ransomware has come encompass a broad set of breach events in which the actors condition the restoration of operations and/or deletion of stolen data on payment of a ransom.
- **Error** – The error category captures all events in which persons with authorized access accidentally disclose sensitive data to unauthorized parties. For example, an administrator storing sensitive data on a publicly accessible S3 bucket.
- **Misuse** – The misuse category contains all events in which a person with authorized access abuses privileges to steal sensitive data or commit fraud.

- **Physical** – Events in the physical category are those in which the primary vector was a physical compromise, such as the theft of a backup tape.
- **Social** – The social engineering events are those in which the compromise was perpetrated using social engineering techniques. The social engineering vector is likely significantly understated as most malware infections originate through a phishing campaign of sorts.

Conclusion

This study of 20,241 publicly reported breach events occurring within 196,000 closely monitored companies from 2015 to 2024 yields numerous valuable insights. First and foremost, it shows just how much the threat pressure has increased, with the number of publicly reported events increasing 450% over the decade at a compound annual growth rate of 16%. During the ten years, 8.1% of companies reported at least one breach event, with the peak year of 2023 seeing 1.8% publicly reporting a breach.

The second startling insight is the stunning growth in the percentage of companies breached in each industry. Every industry has touched a single year breach rate of at least 1%, growing from as low as 0.1% in 2015, as is the case for the utility sector. Energy went all the way to 15.2% a few years ago and healthcare hit 6.7% in 2023. Risk models that use industry-specific breach event frequency data should be updated frequently – things are changing fast.

External and internal threat actors obviously remain active, targeting both enterprises directly and the vendors to whom companies have outsourced systems and services. While no threat actor or breach method can be ignored, the data shows that external threat agents and partners represent a growing dimension of breach events.

Correlating the RiskRecon cybersecurity ratings and assessment data with the breach events, the data clearly shows that companies with good cybersecurity hygiene have dramatically fewer breach events. Companies with good hygiene have a 3.6 times lower frequency of breach events than companies with very poor hygiene. If you are managing supply chain risk, do business with companies that have good cybersecurity hygiene. If you are managing internal cybersecurity, be a business that you would count on to protect your risk interests.

Remember, you can outsource your systems and services, but you can't outsource your risk. RiskRecon makes it easy to understand and act on your third-party cybersecurity risks.

About RiskRecon by Mastercard

RiskRecon by Mastercard 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.