Risk Insights from 10 Years of Breach Event Monitoring of 109,000 Companies

Detailed analysis of 8,892 publicly reported breach events occurring within 109,000 closely monitored companies from 2012 to 2021.

riskrecon.com

sales@riskrecon.com

Table of Contents

Introduction

Welcome to RiskRecon's 10-year study of breach events, spanning the years 2012 – 2021, covering 109,000 closely monitored organizations. Our detailed analysis of these companies and the nearly 9,000 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.

- Between 2012 and 2021, 5.5% of companies publicly reported at least one breach event.
- Comparing 2012 to 2021, publicly reported breach events increased by 314%.
- The peak breach year of the study period was 2020, during which 2.28% of companies publicly reported at least one breach event.
- Healthcare had the highest rate of breach events, with 17.8% of organizations reporting at least one breach during the 10 years. The education sector had the second highest rate, with 17.2% of organizations reporting a breach during the same period.
- Organizations with the largest attack surfaces, having greater than 5,000 internet-facing systems, have a 64 times greater frequency of publicly reported breach events compared with the smallest companies, having 10 or fewer systems in their attack surface.
- Sixty-five percent of breach events are publicly reported within 30 days of a breach.
- Twelve percent of breach events took more than six months to report after the date of the initial compromise.
- Breaches of vendors take 80% longer to report than internal breach events – 4.1 months compared with 2.2 months.
- External actors accounted for 61% of breach events. Internal personnel accounted for 21% of events. Partners accounted for 9%. The remaining were unknown.
- From 2012 to 2021, five of the nine major U.S. holiday windows had a higher breach rate than the average daily breach rate. The days surrounding Veterans Day had the highest holiday-related breach event frequency, running at 253% of the average. Christmas and Thanksgiving also ran hot at 187% and 140% on average.
- The breach event frequency for companies with very clean cybersecurity hygiene ('A-rated' by RiskRecon) was nine times lower than for companies with very poor cybersecurity hygiene ('F-rated' 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.

RiskRecon Risk Management Insights: At the end of each section, we highlight a few key risk management insights derived from the data.

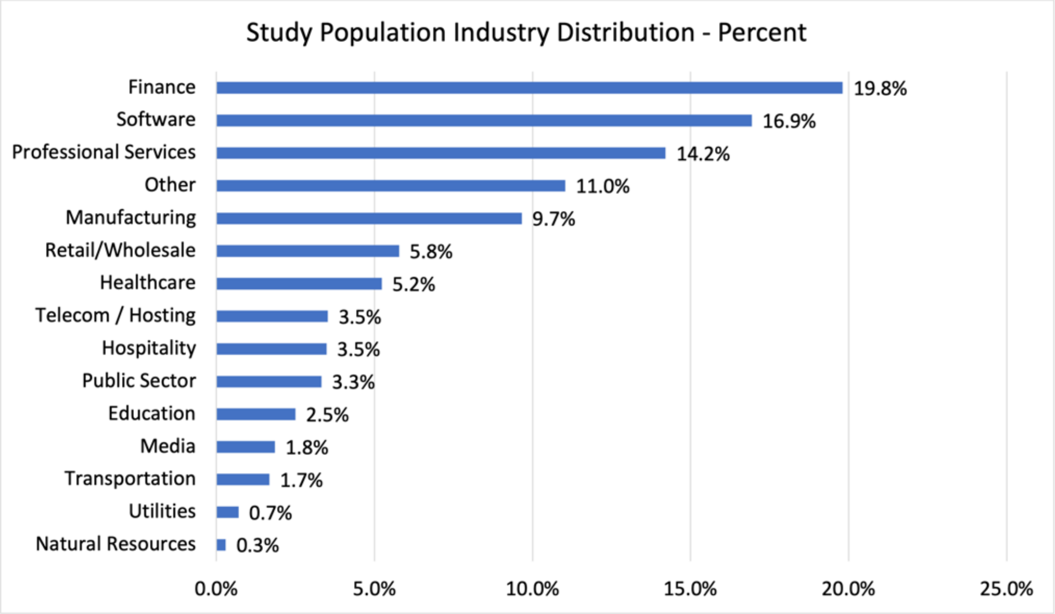
Methodology and Study Population

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, RiskRecon selected 109,000 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, 2012, through December 31, 2021. Analyzing events one year after the end of the study window ensures that nearly all breach events that are going to be publicly reported have been reported. 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.

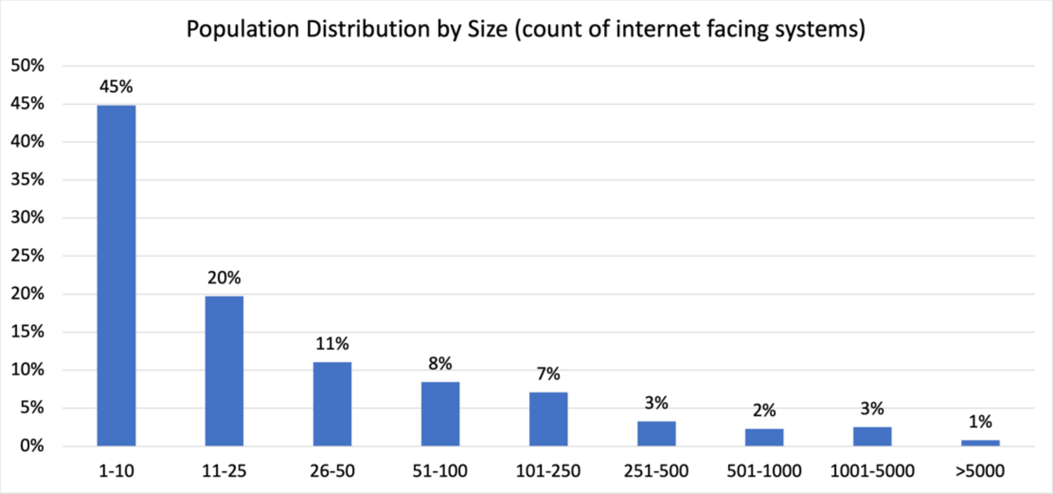
Industries

The study categorizes the organizations into 14 specific industries, with the remaining placed in the category of "other".



Size

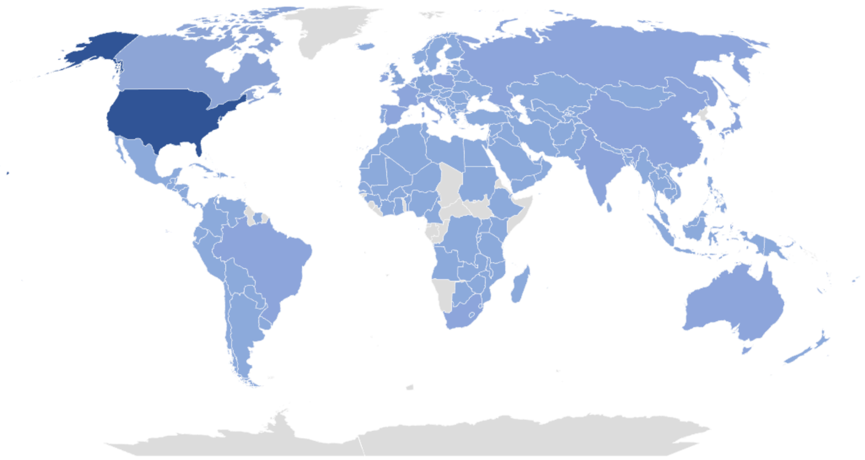
The study population includes companies of all sizes of internet-facing infrastructure. Forty-five percent of companies have 10 or fewer systems in their internet attack surface, while just 1% have more than 5,000.



Geography

The study encompasses companies with primary centers of operation in 191 countries. Most of the organizations are based in the U.S., accounting for 70% of the population. Great Britain and Germany each account for around 3.5%, followed by Canada, Netherlands, and France, each accounting for between 1.5% and 2%.

Geographic Distribution of Monitored Organizations

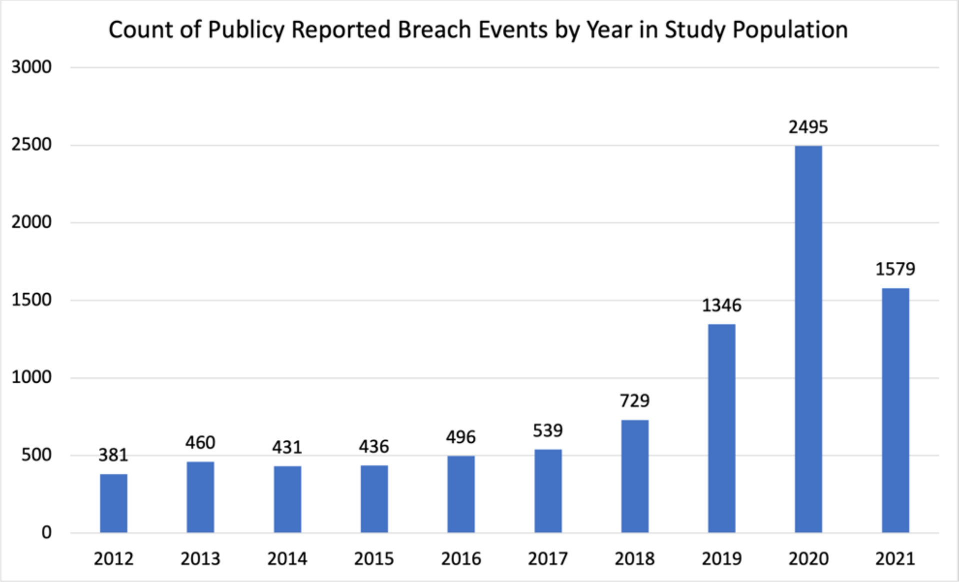


Disclaimer

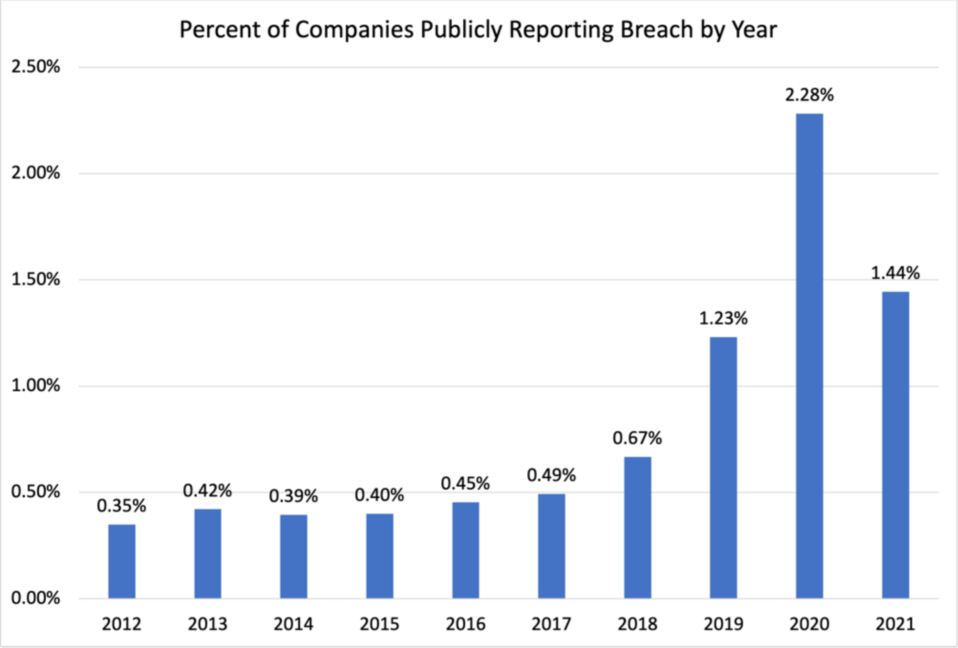
Public breach event notifications are biased and unevenly reported over time. Not all companies publicly report all breach events; it varies based on factors such as geography, industry, the quality of governance, and even the ability to detect a breach at all. Even for countries that now have strict public breach reporting requirements, such as the United States and Europe, the reporting requirements were not as strict in 2012 as they were in 2021. So, we do our best with the data we have.

Top-Level View

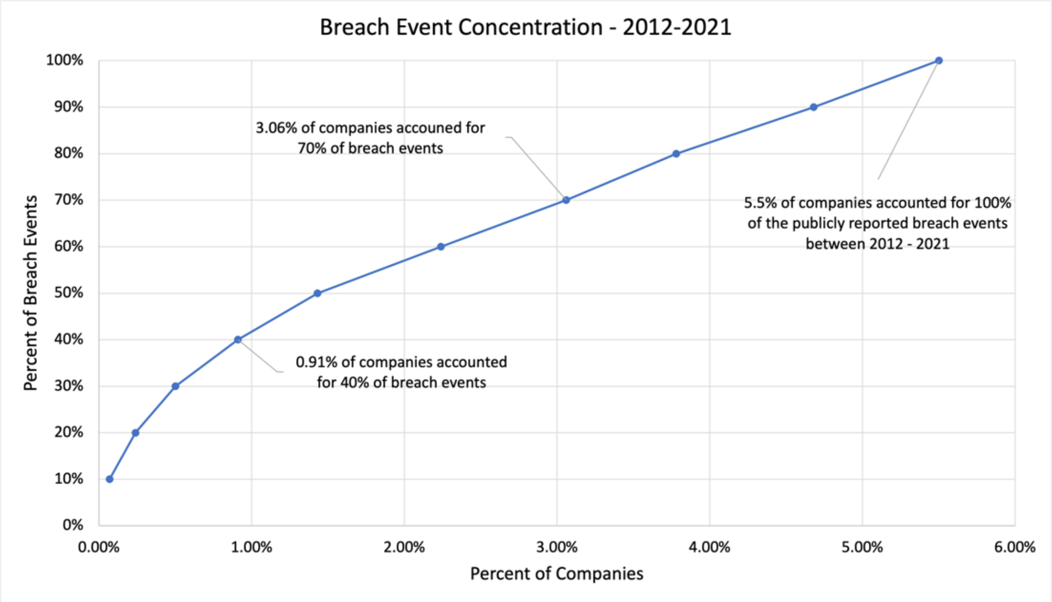
Between 2012 and 2021, RiskRecon analysts identified 8,892 publicly reported breach events within the population of 109,000 organizations. The year 2020 had the highest number of breach events at 2,495. Comparing the first year of the study to the last, publicly reported breach events increased by 314%. With only two exceptions, 2014 and 2021, each year had a higher number of breach events than the previous year.



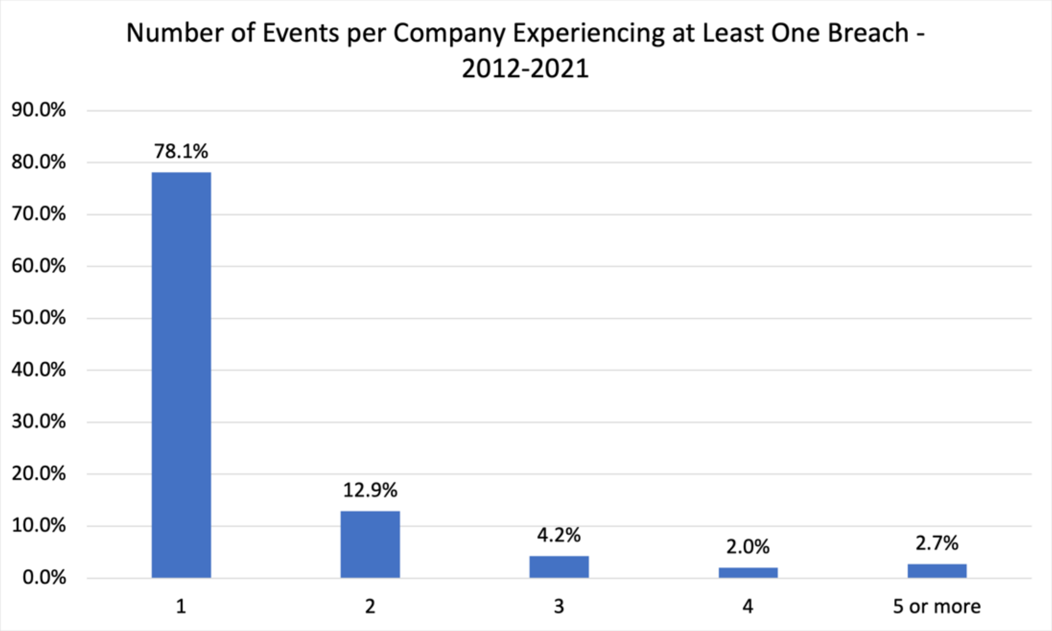
From 2012 through 2021, 5.5% of the companies (6,015) publicly reported at least one breach event – just over 1 in 18. The peak breach event year was 2020, with 2.28% of companies publicly reporting at least one breach. In 2021, the number of companies reporting a breach event was 311% higher than in 2012.



Some companies reported more than one breach event, given that 6,015 companies publicly reported 8,892 events. Three percent of organizations accounted for 70% of breach events, with 2.5% of organizations making up the remaining 30%.



Of the organizations reporting a breach between 2012 and 2021, 78.1% reported one event, while 2.7% reported five or more. Of the top 10 organizations disclosing the highest number of breach events, four were Western governments, three were healthcare organizations, two were social media companies, and one was a software company.

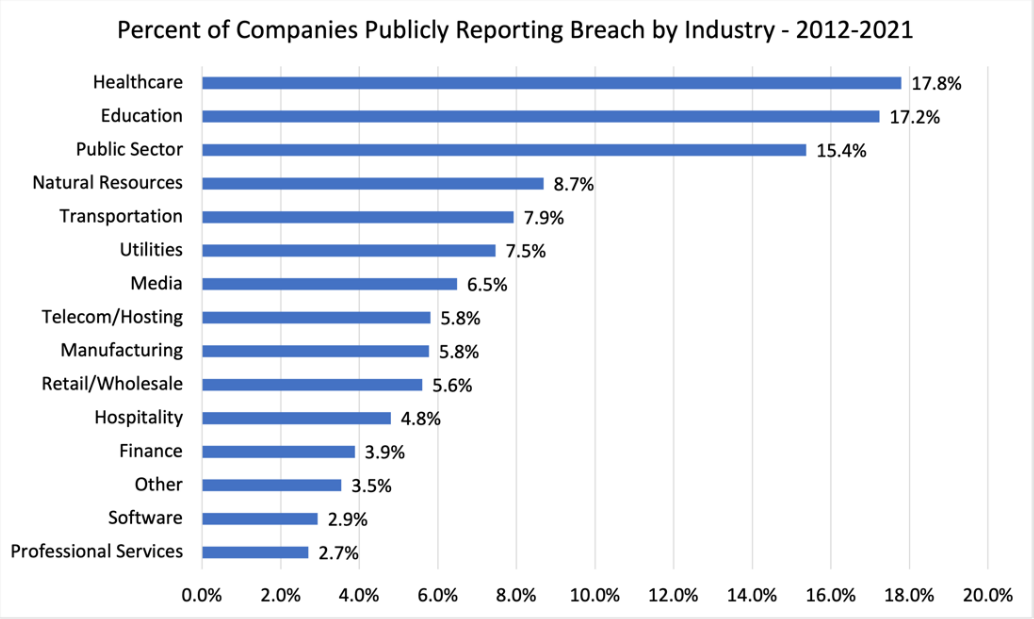


RiskRecon Risk Management Insights: In the peak year of 2020, 2.28% of companies publicly reported a breach event. For those managing third-party risk, this serves as a good baseline for vendor breach volume. At that rate, a portfolio of 500 vendors, which isn't unusual, would have to manage the impact of 11 vendor breach events per year!

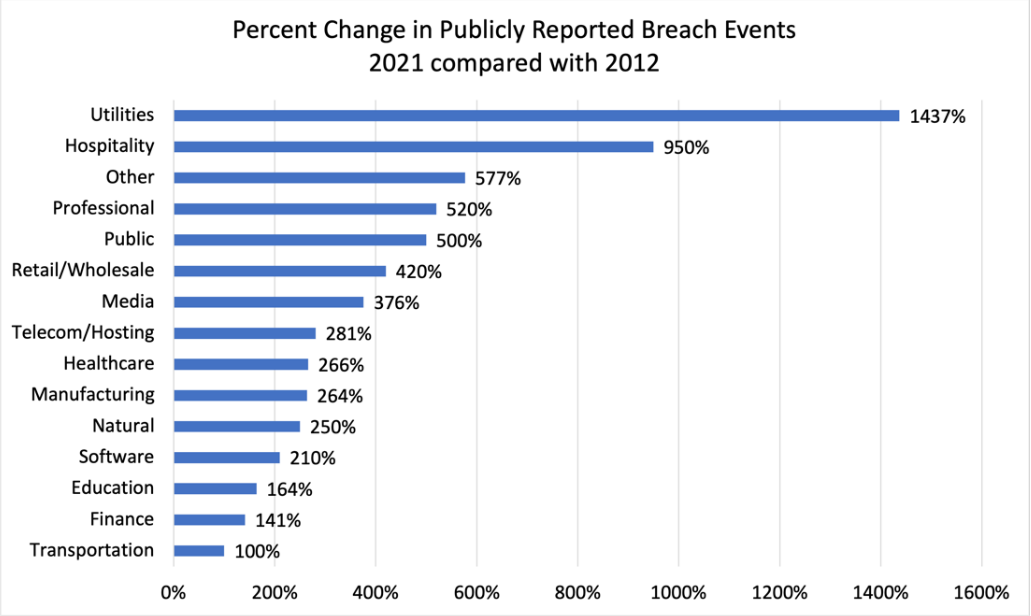
Looking at a longer time horizon, the past 10 years saw 5.5% of all companies publicly report at least one breach event. Going forward, given the increasing threat pressure and the push to move applications, systems, and data to the edge of the enterprise, it is likely we will see even higher rates.

Industry View

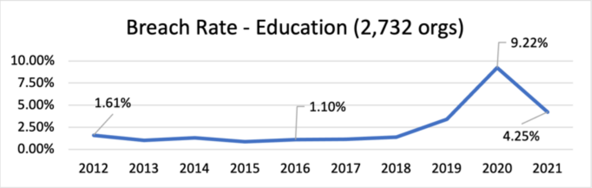
Healthcare and educational institutions reported the highest rate of breach events, with over 17% reporting at least one breach from 2012 to 2021. The public sector didn't fare so well either, with 15.4% of government entities experiencing a breach. On the other end, the finance industry did quite well, considering the massive threat pressure they face, with 3.9% of monitored companies publicly reporting a breach.

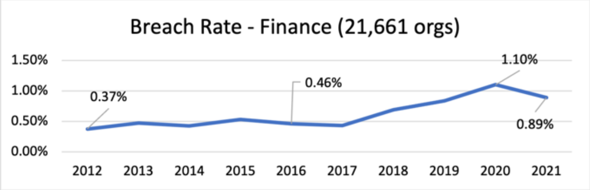


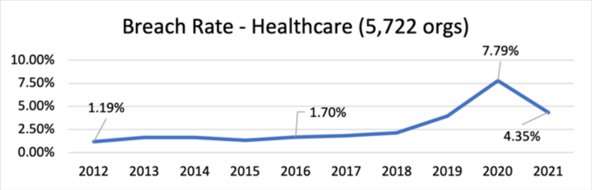
Every industry experienced a higher breach rate in 2021 than in 2012. In 2021, utility companies reported 14 times more compromises than they did in 2012. Hospitality reported 9.5 times more, professional services 5.2 times more, and media 3.7 times more. Indeed, cybercrime has come to roost in industries beyond the traditional favorite target of finance.

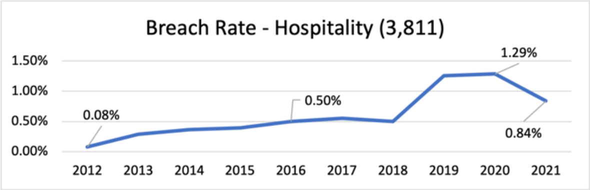


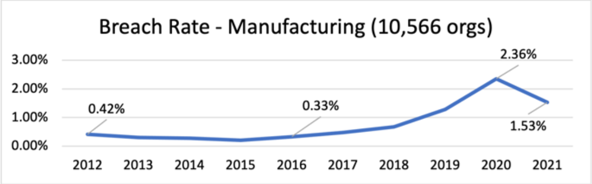
The charts below show the percentage of companies breached each year by industry.

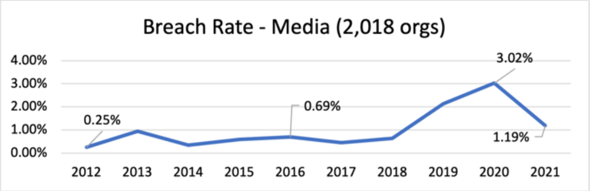

Breach Rate - Education (2,732 orgs)

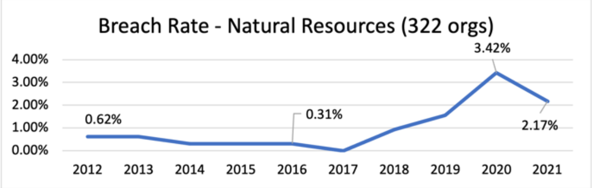

Breach Rate - Finance (21,661 orgs)

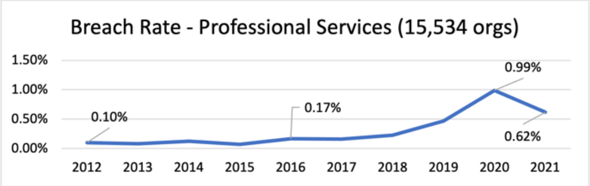

Breach Rate - Healthcare (5,722 orgs)

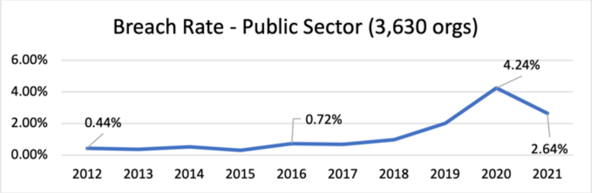

Breach Rate - Hospitality (3,811)

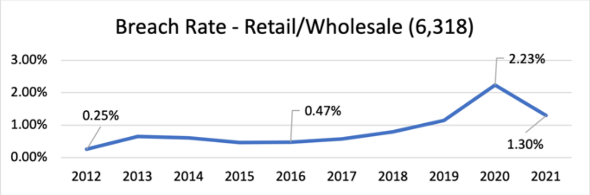

Breach Rate - Manufacturing (10,566 orgs)

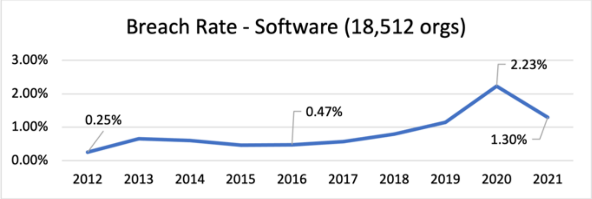

Breach Rate - Media (2,018 orgs)

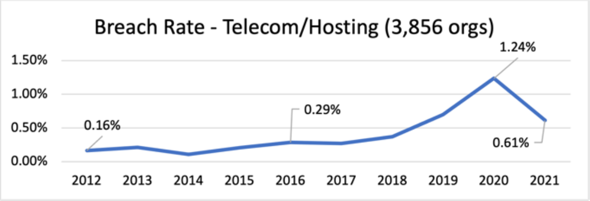

Breach Rate - Natural Resources (322 orgs)

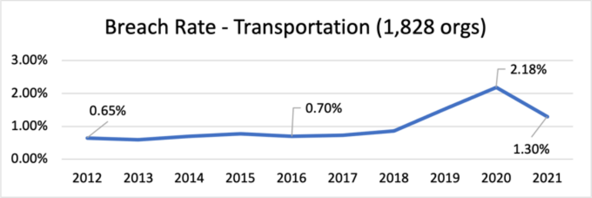

Breach Rate - Professional Services (15,534 orgs)

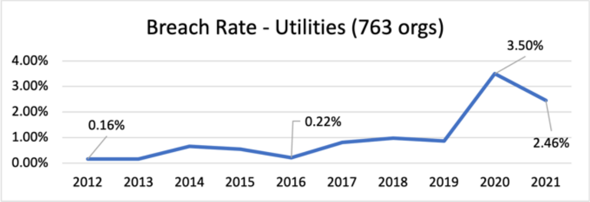

Breach Rate - Public Sector (3,630 orgs)

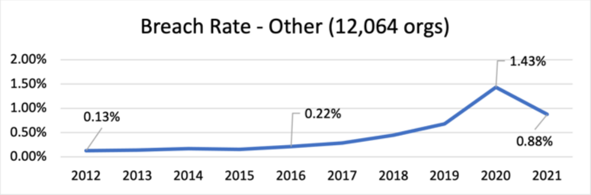

Breach Rate - Retail/Wholesale (6,318)


Breach Rate - Software (18,512 orgs)


Breach Rate - Telecom/Hosting (3,856 orgs)


Breach Rate - Transportation (1,828 orgs)


Breach Rate - Utilities (763 orgs)

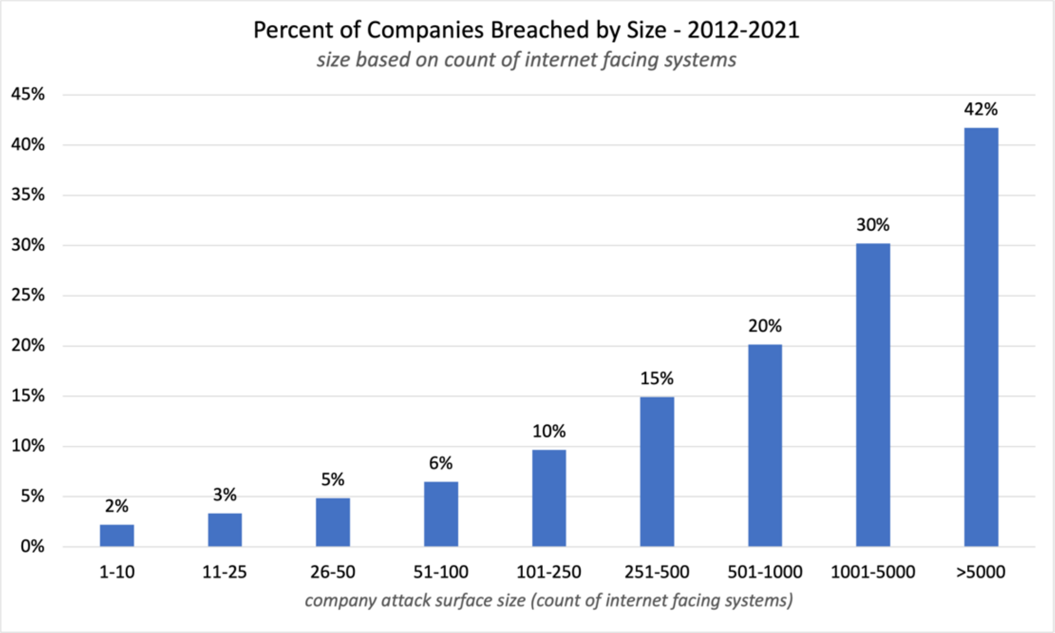

Breach Rate - Other (12,064 orgs)

RiskRecon Risk Management Insights: Industry sectors that were largely ignored 10 years ago are now publicly reporting breaches more frequently than traditional targets. Utilities, hospitality, education, professional services, governments, and media all had at least a 300% increase in publicly reported breach events. The utility industry went from a breach rate in 2012 of 0.16% to 3.5% in 2020!

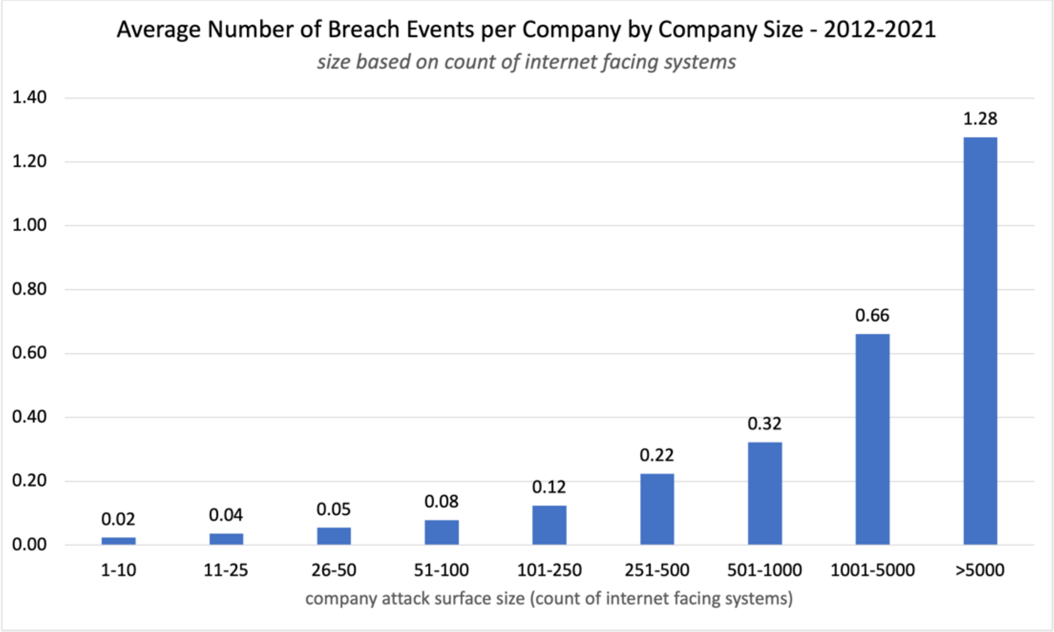
Risk managers would be wise to update their industry-specific cybersecurity risk models. Those using old data will dramatically underestimate breach event frequencies.

Company Size View

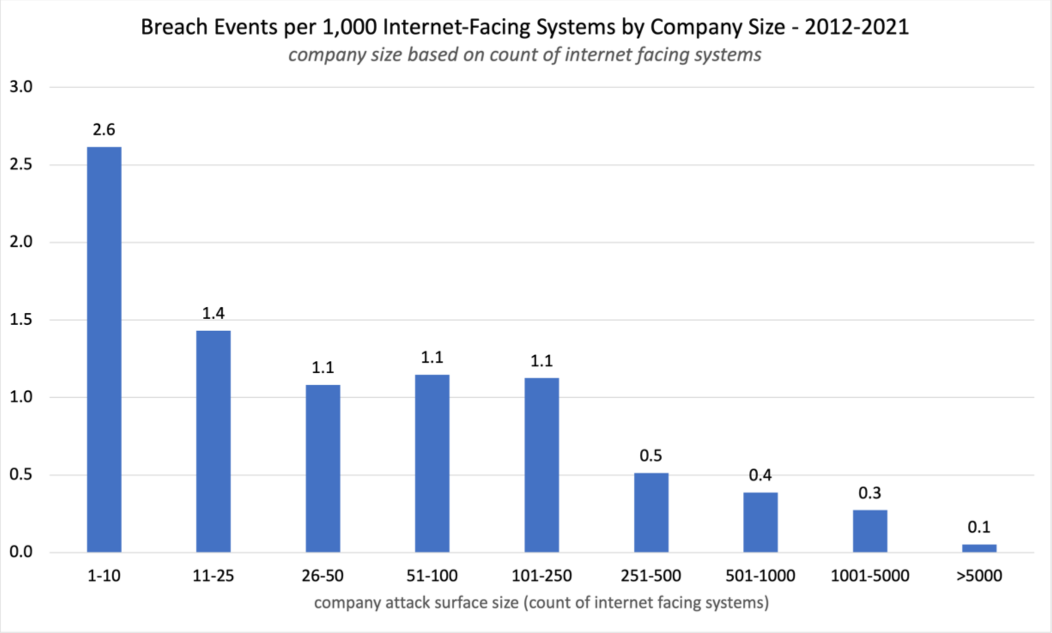
One of the best predictors of breach event frequency may be the size of the organization's attack surface – the number of systems the company operates on the internet. The larger an organization's internet presence, the higher the frequency of breach events. Looking at the extremes, organizations with greater than 5,000 internet-facing systems had 21 times higher publicly reported breach events than companies with 10 or fewer systems.



Companies with the largest attack surfaces publicly reported an average of 1.28 breach events from 2012 to 2021, 64 times higher than the smallest organizations.



Stopping there, one might conclude that companies with larger attack surfaces are less competent in protecting their systems. However, from the perspective of breach events per 1,000 systems, that is not the case. The larger the attack surface, the lower the number of breach events per 1,000 systems.



The net of it is that companies with the largest attack surfaces are breached 64x more frequently than the smallest organizations, so they are going to drive a lot of third-party incident response. However, that doesn't mean the largest organizations are less competent. In fact, on a per-system basis, they are comparatively very good at protecting systems; they are just having to protect such a massive infrastructure.

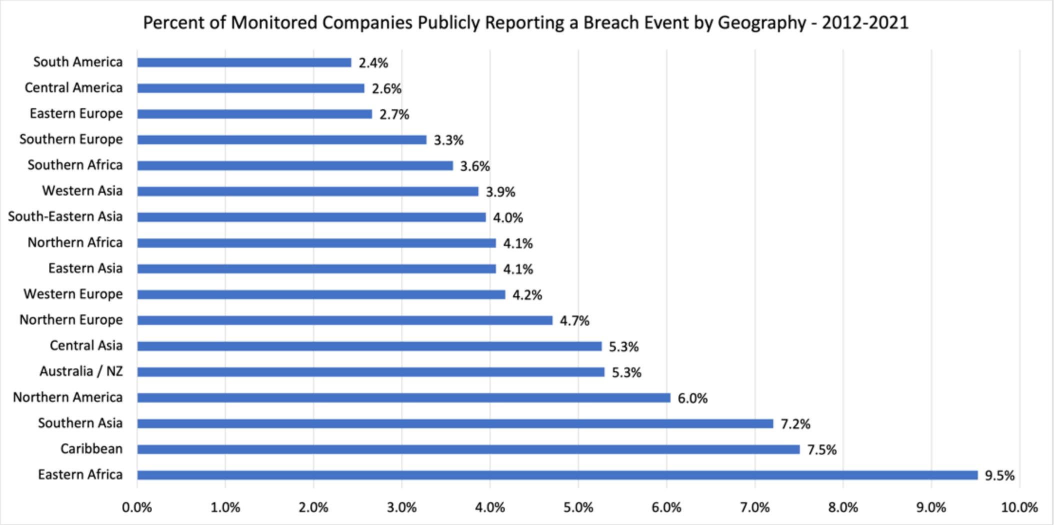
RiskRecon Risk Management Insights: If you are managing third-party risk, you would be wise to factor the size of the organization's attack surface into your inherent risk model. The larger the attack surface, the higher the breach event frequency. Companies with >5,000 systems in their attack surface have a 64x 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.

Geography View

Meaningful analysis of geographic-specific breach events is difficult. Regional factors like regulations and cybersecurity capability strongly influence the number of breach events that are discovered and reported. The degree of targeting of companies in each region also influences the data.

Highlighting this reality, our analysis shows that about 2.5% of monitored companies in South America and Central America publicly reported a breach event between 2012 and 2021. In comparison, 6% of monitored companies in North America reported a breach. Does this mean that companies in North America have worse cybersecurity than companies in South and Central America?

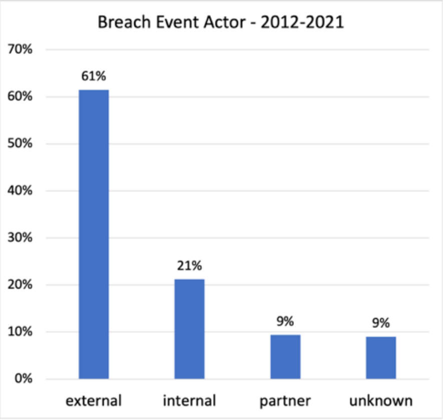


So, what can we conclude based on this geographic breach frequency data? Well, perhaps the following are worth thinking about:

- 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 10-year breach rate. That is 4.2% on the low end (Western Europe) and 6% on the high end (North America).

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.

Breach Actors

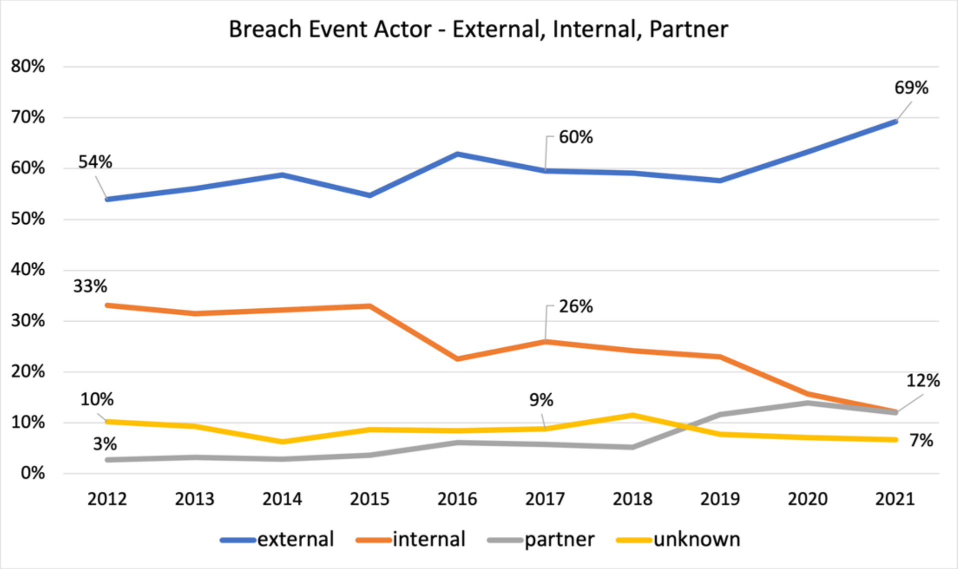


For 91% of the breach events, the public notifications disclosed the general threat actor. From 2012 through 2021, 61% of breach events were attributed to external threat actors, followed by 21% attributed to internal actors, and 9% to partners. The trend data tells a rapidly evolving story, with larger percentages attributed to external actors and partners, and a decreasing portion attributed to insiders over time.

External actors, outsiders compromising the systems of an organization, have always been the absolute majority, growing from 54% of breach events in 2012 to 69% in 2021. No doubt, the ability to monetize breaches through crypto-based ransom demands fueled this growth.

In terms of growth rate, breaches of partners/vendors took the top spot, growing 300% between 2012 and 2021. Given the massive amount of outsourcing of systems and services, it is reasonable to expect to see vendor breach events continue to grow at a high rate.

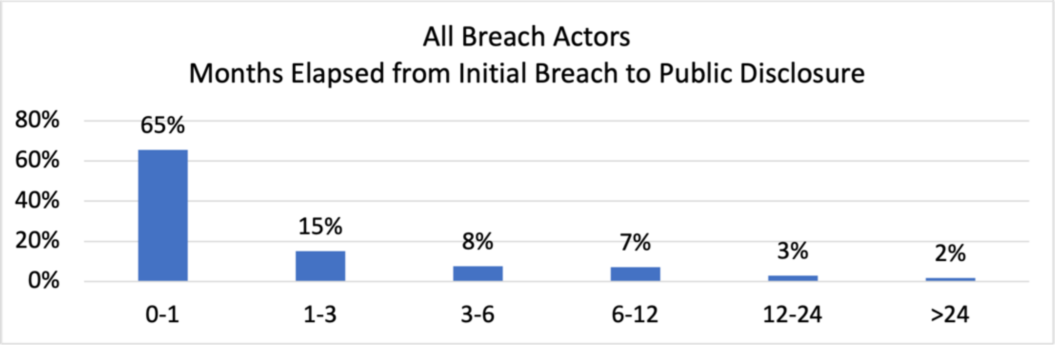
Relative to other actors, insider-driven events were subdued, reaching a low in 2021 of 12% of all events. This is a decrease from the high-water mark in 2012 when insiders were behind 33% of all events. Keep in mind, while insider activity decreased relative to the total events, insider breach events still increased by 50% over the 10 years.



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 2021 was higher than in 2012. 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

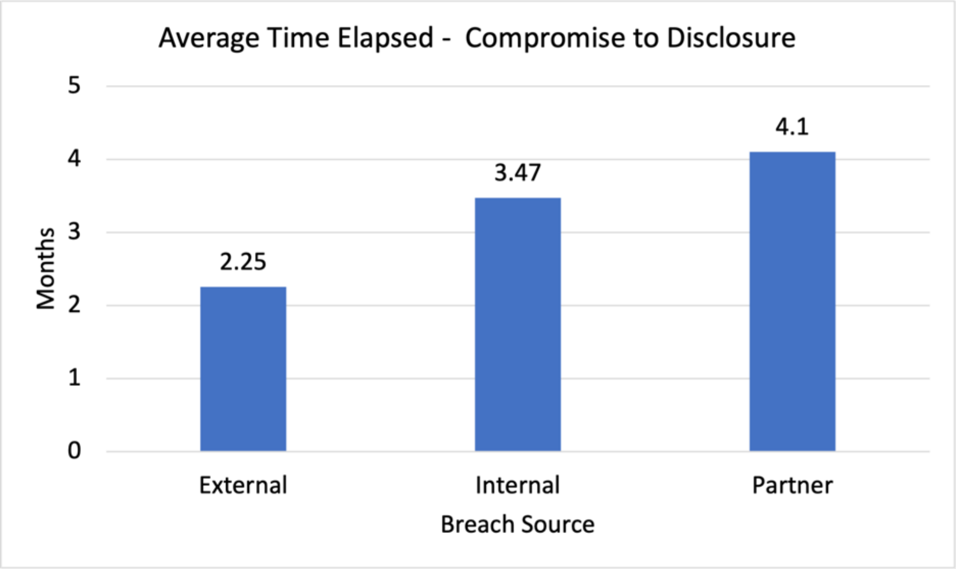
For 80% of events, the time between initial compromise and disclosure is less than three months. This seems reasonable given some days to detect the event, followed by weeks to investigate, and then work with legal and PR to formulate and submit the necessary filings and disclosures.



The events of particular interest are the 5% 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:

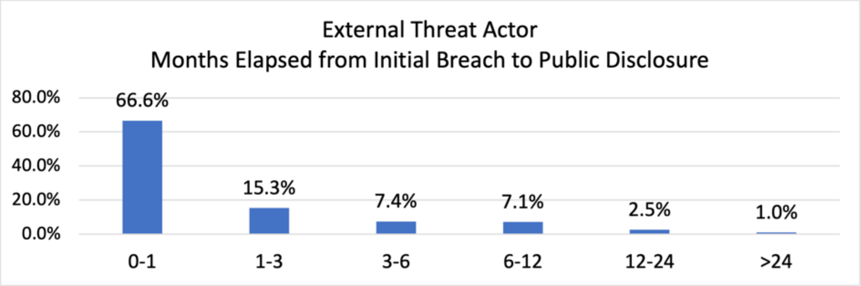
- "[Company] has discovered its web hosting provider failed to patch vulnerabilities which were exploited by cybercriminals to gain access to its website and protected health information of applicants for benefits for the past seven years."
- "Healthcare Provider Discovers Patient Data Exposed Online for Over Four Years"
- "After thorough investigation, it was determined that the employee improperly accessed certain patient information between October 2009 and February 2019."

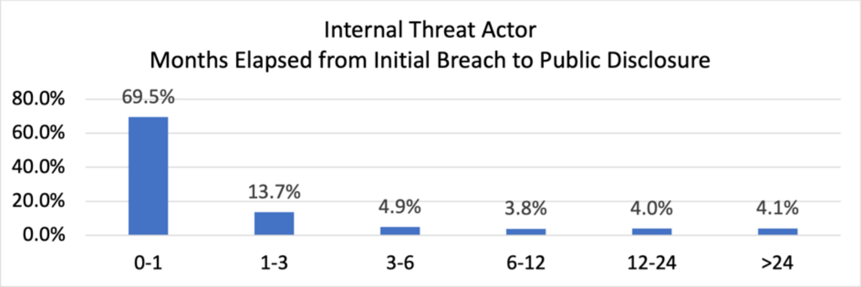
Disclosure of breach events rooted in compromise of a partner took the longest to disclose, averaging 4.1 months. Insider breach events took 3.5 months to disclose, 54% longer than compromises by external actors which averaged 2.25 months.

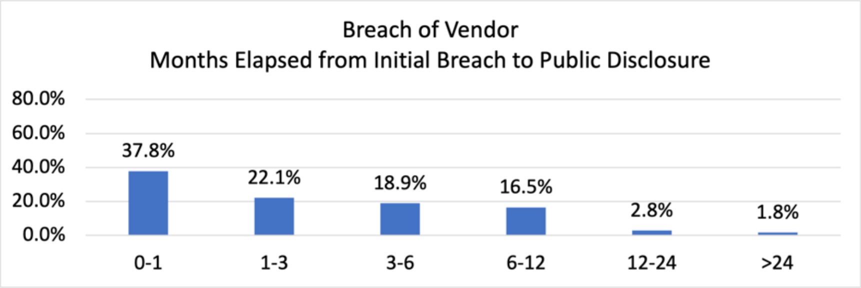


The problem of timely partner-related breach event reporting is magnified when examining the disclosure time distributions by actor. For breaches occurring within their own environment, companies disclosed 68% of events within one month of the initial compromise. In contrast, for breaches rooted in the compromise of a vendor, companies only disclosed 38% of breach events within one month.

Twenty-one percent of the vendor breach events took longer than six months to disclose. In comparison, only 11% of breach events in an organization's own environment took longer than six months.







RiskRecon Risk Management Insights: Risk managers should take serious notice of the lags in publicly disclosing vendor-related breach events. Only 38% were reported within 30 days of the breach, in comparison with 68% for all other sources. Even worse, 28% of those vendor breaches took six months or longer to disclose. That is a lot of time for criminals to freely leverage your stolen assets and puts you at risk of violating breach disclosure notification rules.

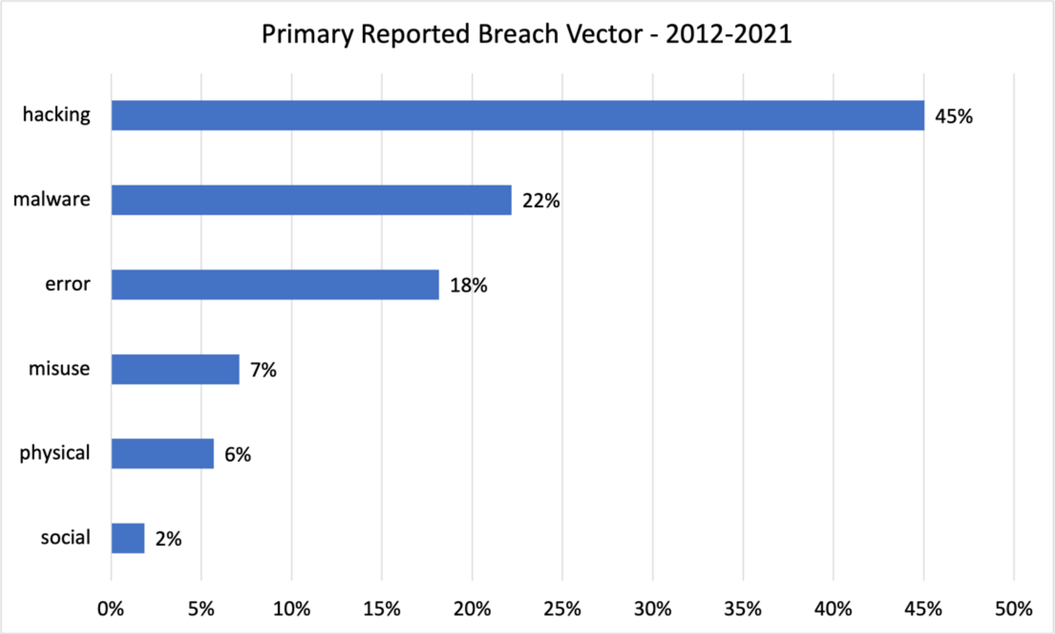
There is clearly room to improve vendor-related breach notifications. Perhaps there needs to be better lines of communication between customers and vendors and tighter vendor SLAs on reporting breach events. Perhaps companies would be wise to expand their own deep and dark web monitoring to detect breaches of their vendors.

Breach Vectors

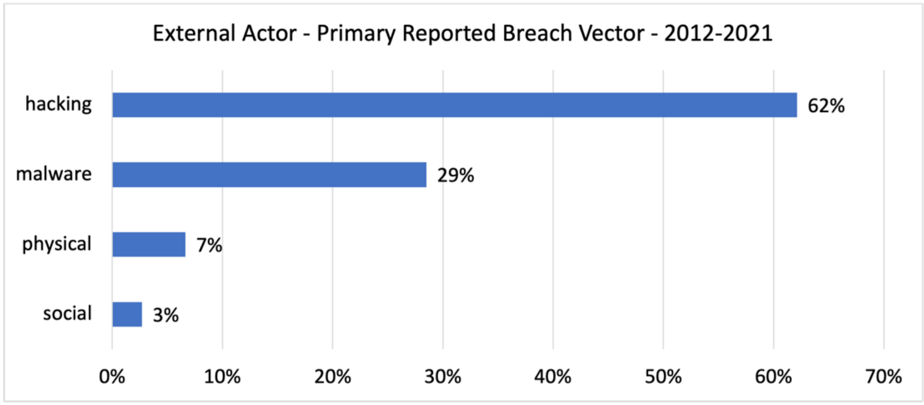
The primary compromise vector was publicly reported for 85% of breach events, though often in generic terms. RiskRecon categorized the vectors into six groups:

- 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, including ransomware, deployed to endpoints and servers.
- 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.

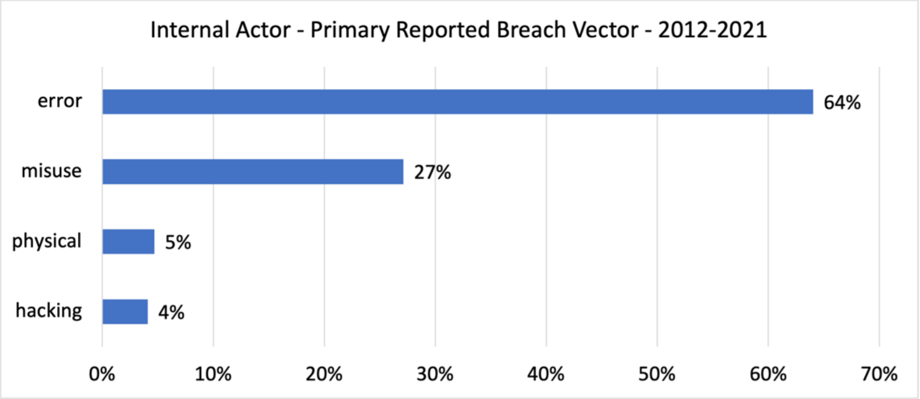
Hacking was the top vector referenced in public notifications, representing 45% of all breach events. Malware was cited in 22% of the cases, followed by employee error at 18% and employee privilege misuse at 7%. Social engineering was cited in only 2% of breach notifications, but this is very likely vastly understated as a large percentage of malware infections and credential thefts occur through phishing.



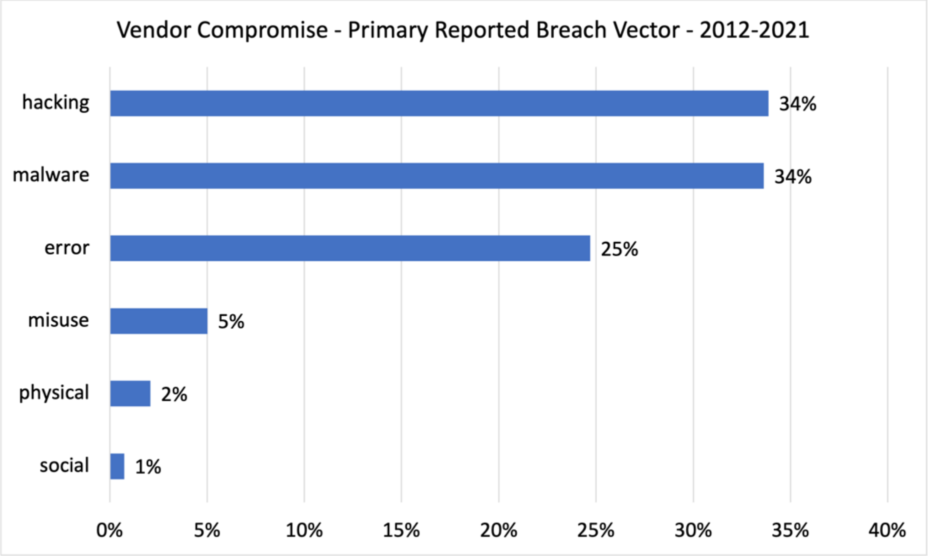
Different threat actors leverage different techniques. External actors are cited as hacking in 62% of the cases and as deploying malware in 29%.



For internal actors, an error is cited as the leading cause at 64%, followed by misuse/privilege abuse in 27% of the breach events.



In vendor breach events, we see a mix of the insider and external vectors, where hacking and malware both come in at 34% and employee error comes in at 25%.

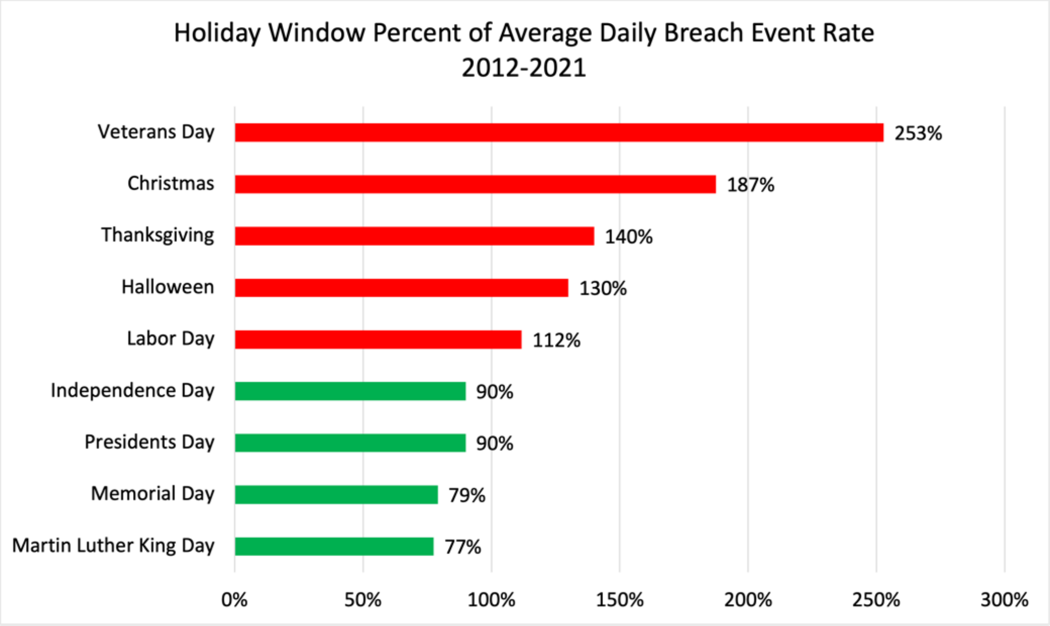


U.S. Holiday Breach Event Frequency

The exact date of the initial compromise was documented in 13% (1,217 of 8,892) of the public breach notifications. At the risk of being overly descriptive, we measured the frequency of breach events occurring during the windows of major U.S. holidays during the 10-year period by:

1) Building a single-year calendar containing the holiday windows for the years 2012-2021. This is necessary because some holidays, such as Thanksgiving, vary in date from year to year. The holiday window was constructed to contain three days before and three days after each official holiday, accounting for vacation time surrounding each holiday.
2) Assigning all breach events to the month/day date that they occurred. For example, all events occurring on July 21 throughout the 10 years were assigned to July 21 on the single-year breach calendar.
3) Comparing the breach event frequency for holiday windows with that of the average day in the single-year breach calendar.

The data shows that five of the nine major U.S. holiday windows have a higher breach rate than the average daily breach rate. 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.

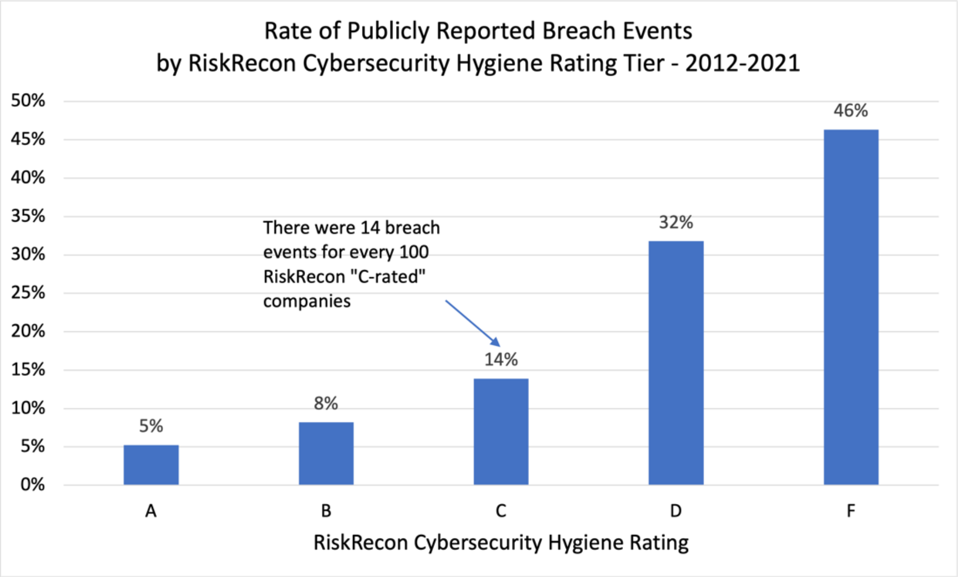


RiskRecon Risk Management Insights: There are no breaks for the information security teams. Criminals are increasing their compromise campaigns on many of the major holidays. Particularly, maintain your capabilities at 100% for the holiday windows of Veterans Day, Christmas, Thanksgiving, Halloween, and Labor Day.

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.

Companies that have very poor cybersecurity hygiene in their internet-facing systems (a 'D' or 'F' RiskRecon rating) have a seven times higher frequency of breach events in comparison with companies that RiskRecon observes to have very good cybersecurity hygiene (an 'A' RiskRecon rating). As shown in the chart below, the rate of breach events for 'A-rated' companies is 5 for every 100 companies from 2012-2021, compared with 32 for every 100 'D-rated' companies and 46 for every 100 'F-rated' companies.



Looking underneath the ratings, the assessment data shows a stark contrast in average cybersecurity conditions of breached organizations compared with the general population. Those that publicly reported a breach event between 2012 and 2021, on average, have:

- 6.5 times more high and critical severity issues in their internet-facing systems.
- 8.7 times more unsafe network services exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.
- 10.5 times higher rate of malicious activity such as botnet communications emanating from their systems to the internet.
- 6.7 times higher count of web applications that collect sensitive data that has HTTP encryption issues such as expired certificates, weak encryption algorithms, or invalid certificate subjects.

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

	Average Issue Count		
	Breached Company	General Population	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	12.4	1.9	6.5x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	37.2	4.3	8.7x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	21.6	3.8	6.7x 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.	10.5	1.0	10.5x higher

Ignoring issue counts and just looking at the percent of companies with one or more issues across the cybersecurity domains, the companies publicly reporting a breach between 2012 and 2021 stand out as having very poor hygiene in comparison to the general population. In comparison with the general population, the breached company population has:

- 2.3 times more companies with at least one high or critical severity software vulnerability in their internet-facing systems.
- 1.7 times more companies with at least one unsafe network service exposed to the internet.
- 5 times more companies with at least one system exhibiting malicious activity such as botnet communications.
- 1.6 times more companies with at least one sensitive web application that has HTTP encryption issues such as expired certificates, weak encryption algorithms, or invalid certificate subjects.

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

	Percent with at Least One Issue		
	Breached Company	General Population	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	41%	18%	2.3x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	48%	29%	1.7x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	63%	39%	1.6x 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.	10%	2%	5.0x higher

No doubt, 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 seven 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.

Conclusion

This study of 8,892 publicly reported breach events occurring within 109,000 closely monitored companies from 2012 to 2021 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 314% over the decade. The peak breach year, 2020, was 505% higher. During the ten years, 5.5% of companies reported at least one breach event, with the peak year seeing nearly 2.3% reporting.

The second startling insight is the stunning growth in the percentage of companies breached in each industry. Industries such as utilities, hospitality, and natural resources, which were previously passed by are now common targets. 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. And the data shows that threat actors do not rest on major holidays, requiring enterprises to maintain their guard 24x7x365.

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 cybersecurity hygiene have a seven 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, a Mastercard Company

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.