OCTOBER 2023

TRENDS IN CYBERSECURITY BREACH DISCLOSURES

A 12-YEAR REVIEW

2011 - 2022

www.AuditAnalytics.com

Ideagen
Audit Analytics

TABLE OF CONTENTS

INTRODUCTION

The importance of cybersecurity has become more paramount for businesses as the reliance on technology has integrated into daily life. The amount of data transmitted during the digital age of information and technology has grown rapidly, far outpacing technological regulations imposed by the Securities and Exchange Commission (SEC).

Companies must install information security systems and monitor cybersecurity controls to protect vulnerable data from breaches or attacks. Adding to these concerns, cybersecurity threats are becoming increasingly advanced.

However, disclosure guidelines vary widely depending on location, industry, and regulatory agency overseeing the entity. As a result, there are differences in the amount of information provided across breaches. In general, disclosures about cybersecurity incidents may include breach type, information compromised, timeframes and costs.

Currently, SEC disclosure requirements under Regulation S-K and Regulation S-X do not specifically refer to cybersecurity events. Although, the requirements, and subsequently issued guidance, do impose an obligation to disclose certain types of risks and incidents that could have a material impact, including a cybersecurity incident.[1]

On July 26, 2023, the SEC adopted final rules requiring and standardizing disclosures for material cybersecurity incidents for public companies. Periodic disclosures of a registrant's cybersecurity risk management, strategy, and governance are now required in annual reports. Disclosures of material cybersecurity incidents are also now required in Form 8-K for US based registrants and in Form 6-K for foreign issuers. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.

These rules include:

- Current reporting about material cybersecurity incidents in an Item 1.05 of an 8-K, and periodic reporting on incident updates;
- Periodic reporting about cybersecurity policies, procedures, and risk; the oversight role of the Board of Directors in regard to cybersecurity risks; and management's role and expertise with cybersecurity matters;
- Cybersecurity disclosures must be made using inline XBRL.

The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K and Form 6-K disclosure requirements will take effect on December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure.[2]

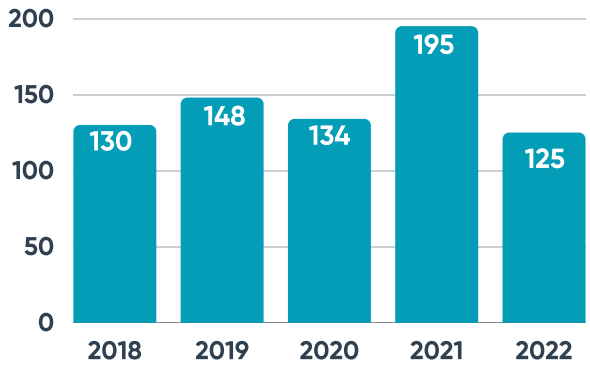
1 Securities and Exchange Commission (February 21, 2018). SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/news/press-release/2018-22
2 Securities and Exchange Commission (July 26, 2023). SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2023-139#

EXECUTIVE SUMMARY

The number of cybersecurity breaches disclosed in 2022 decreased by 36%.

1

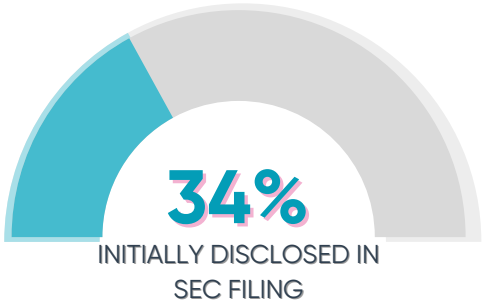
In 2022, 125 breaches were disclosed by public companies. This is the sharpest decline in disclosures seen over the 12-year period.



Less than half of cybersecurity breaches were initially disclosed in an SEC filing.

2

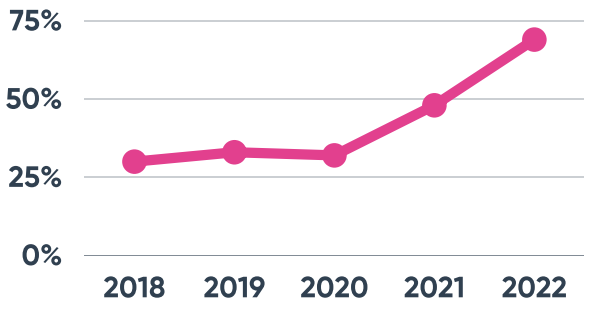
In 2022, 34% of cybersecurity incidents were initially disclosed in a filing with the SEC. Most commonly, the disclosure appeared in an 8-K or 6-K current report.



Unauthorized access contributed to 69% of breaches disclosed in 2022.

3

The percentage of disclosed cybersecurity breaches related to unauthorized access increased to 69% in 2022 from 48% in 2021.



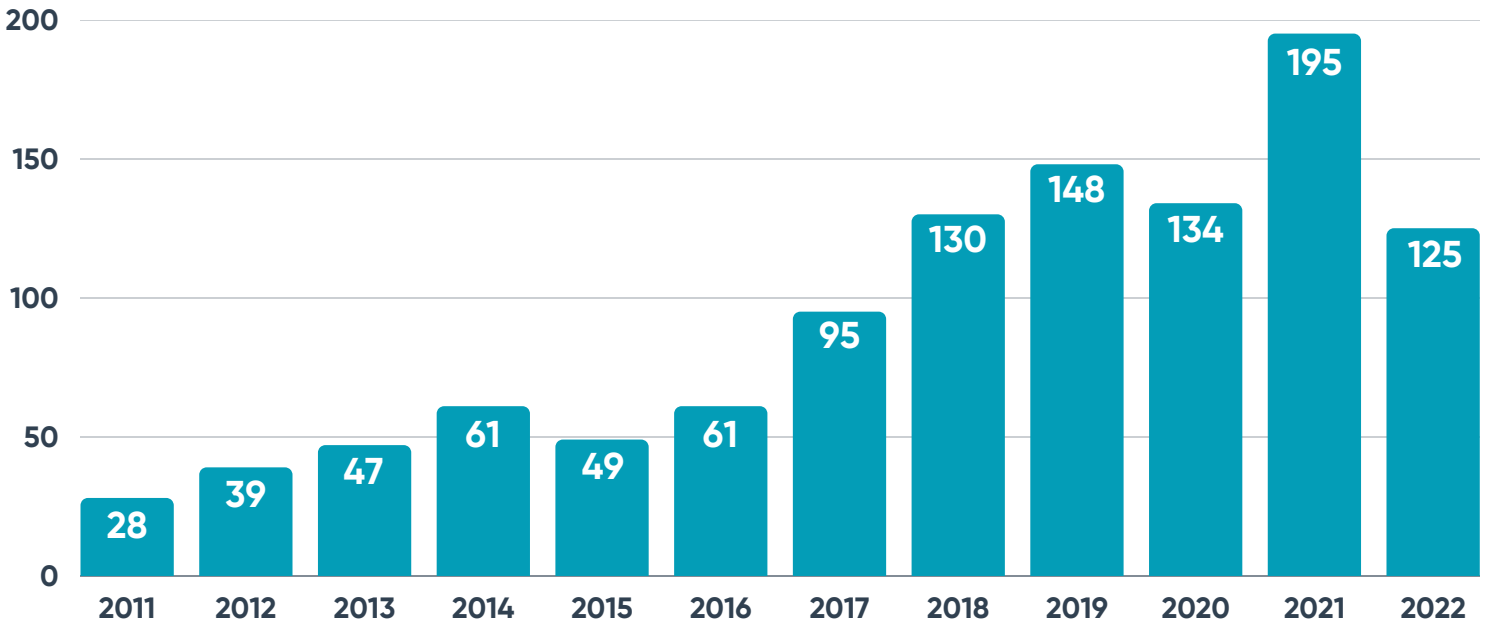
On average, companies took 96 days to disclose a breach after it was discovered.

4

In 2022, companies averaged 96.2 days to disclose a breach after it was discovered. In 2021, the average disclosure window was 78.9 days, almost 2.5 weeks shorter.

OVERVIEW

Total Cybersecurity Breach Disclosures



The total number of cybersecurity breach disclosures declined to 125 incidents during 2022, representing a 36% decrease from the prior year. In 2022, there were only 111 public companies out of over 7,000 SEC registrants that reported a cybersecurity incident.

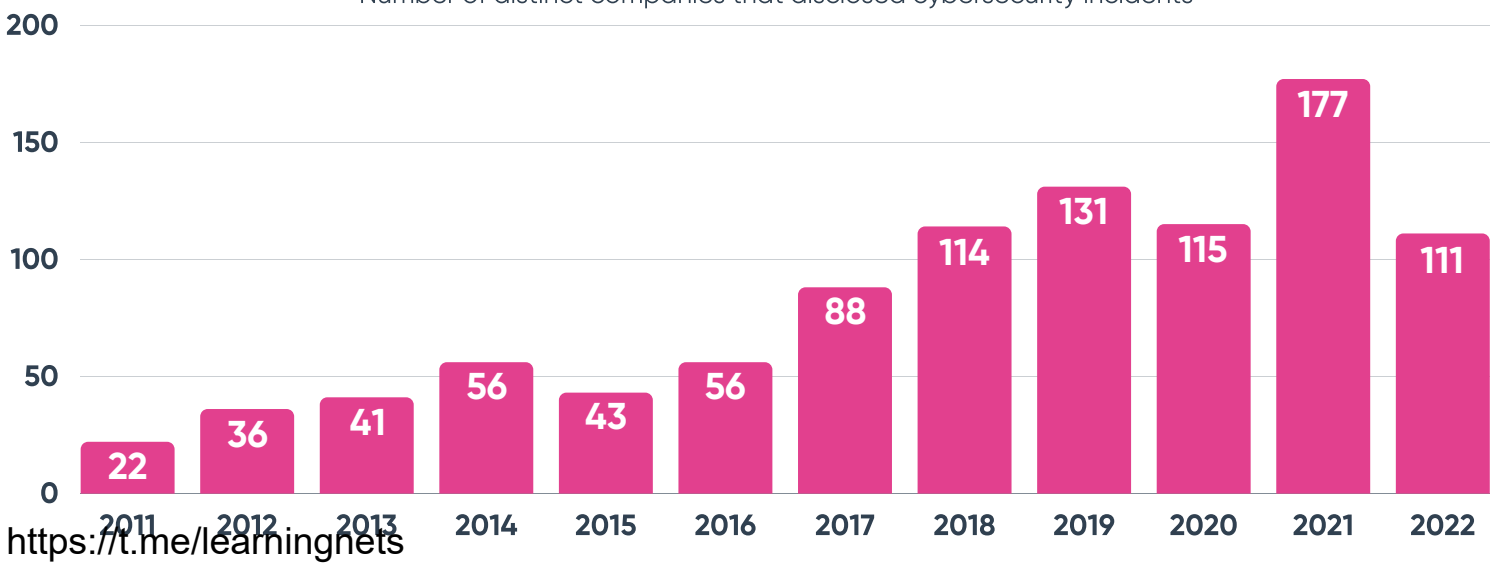
Between 2020 and 2021, the number of cybersecurity incidents increased by 45.5%, reaching an all-time high in total breach disclosures. Similarly, the number of companies impacted by cybersecurity incidents rose 54% to a record high of 177 companies in 2021.

Despite slight decreases in 2015 and 2020, the number of cybersecurity incidents has been slowly rising each year. Compared to 2011, the number of annual disclosed cybersecurity incidents has increased by 346% in 2022.

The SECs newly established reporting requirements are expected to have an impact on the number of public company cybersecurity dsiclosures. These changes are expected to alter disclosure trends in the years to come.

Total Number of Public Companies

Number of distinct companies that disclosed cybersecurity incidents

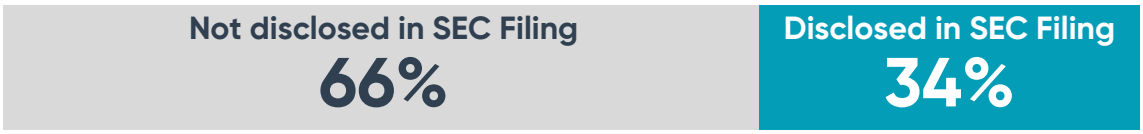


METHOD OF DISCLOSURE

As mentioned in the Introduction, there were limited provisions that required public companies to disclose cybersecurity breaches prior to the newly adopted changes in SEC disclosure requirements. Sources of cybersecurity incident disclosures outside of SEC filings include press coverage and notifications from state attorney generals' offices.

Of the 125 cybersecurity incidents that were disclosed in 2022, 34% were initially discussed in an SEC filing. Companies that did not initially disclose the incident with the SEC may later release a filing discussing the breach.

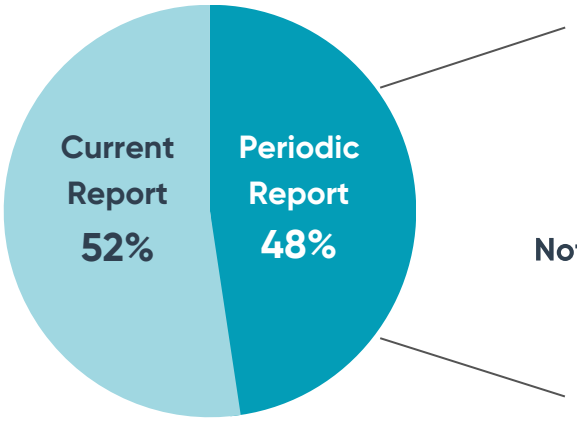
2022 Cybersecurity Breach Initial Disclosures



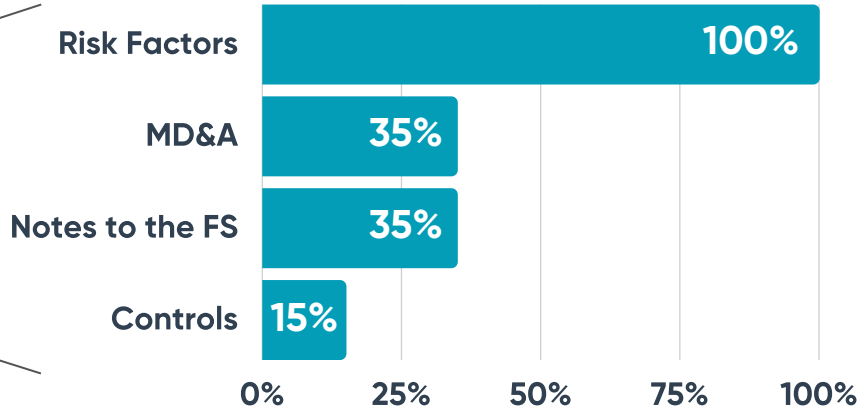
In 2022, the majority of companies that initially disclosed a cybersecurity breach in an SEC filing did so in an 8-K or 6-K (current report), representing 52% of all initial SEC breach disclosures.

2022 SEC Initial Disclosures

SEC Filing Type



Periodic Report Location



Within a company's periodic filings (10-K or 10-Q), cybersecurity breach disclosures can be found in multiple locations. All of the initial periodic report disclosures were included in the Risk Factors section. Initial disclosures were also found in Managements Discussion & Analysis and the Notes to the Financial Statements, each representing an additional 35%. Only 15% of initial disclosures discussed the cybersecurity breach as it relates to the company's internal controls.

TYPE OF CYBERSECURITY BREACHES

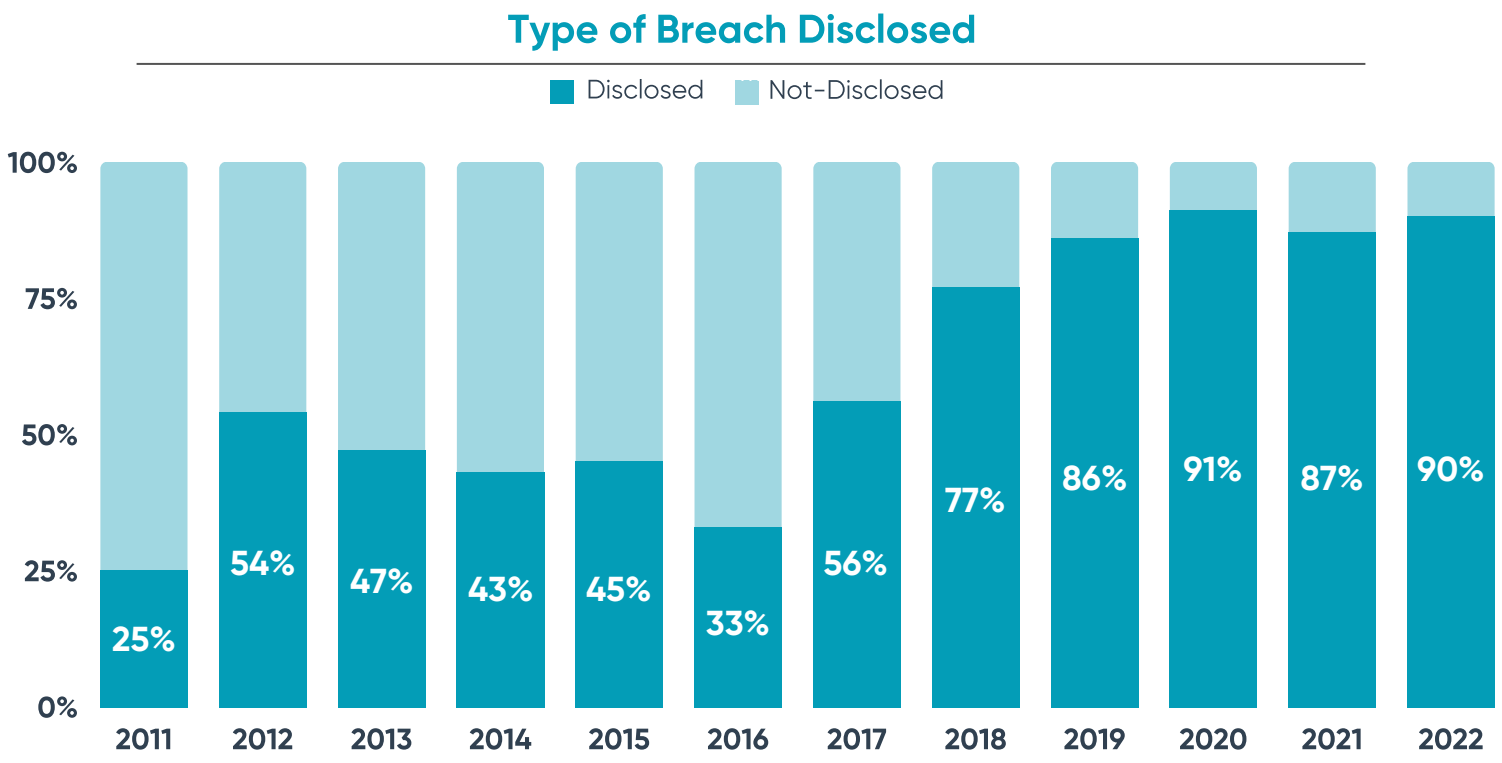
Breaches that allowed an incursion into company systems can be attributed to different types of attacks: unauthorized access, phishing, misconfiguration, malware, and ransomware.

Type of Breach	Description
Unauthorized Access	Unauthorized party gains access to protected systems and data
Phishing	Fraudulent attempt to obtain sensitive information under guise of trustworthy electronic communication
Misconfiguration	Exploitation of incorrectly assembled code, safeguards and web applications
Malware	Malicious software intentionally designed to cause damage
Ransomware	Specific type of malware designed to hold systems hostage in exchange for demands being met

Despite the lack of standardized cybersecurity disclosure requirements, most companies that disclosed cybersecurity incidents also disclosed the type of breach that occurred.

Overall, since 2011, 72% of cybersecurity incident disclosures specified the type of attack used to penetrate a company's systems.

In 2022, 90% of cybersecurity breach disclosures specified the type of attack used. Since 2017, there has been an upward trend in disclosing the method of cybersecurity attack. At the low point in 2011, only 25% of disclosures listed the type of attack.



Since 2011, the most common cybersecurity attack method has been unauthorized access, contributing to 36% of total disclosed breaches. The second most common type of breach since 2011 has been malware incidents, contributing to 21% of total disclosed attacks.

Overall: 2011-2022		
Type of Attack	% of Disclosed Breaches	# of Breaches
Unauthorized Access	36%	287
Malware	21%	166
Phishing	18%	145
Ransomware	15%	120
Misconfiguration	11%	91

In line with the overall trend, the most common type of cybersecurity breach in 2022 was unauthorized access, contributing to 69% of total disclosed attacks. Conversely, malware attacks contributed to only 3% of total disclosed attacks in 2022, a significant decrease from the overall trend.

Ransomware attacks were the second most common type of cybersecurity breach in 2022, contributing to 17% of incidents disclosed during the year. In comparison to the overall trend, ransomware has become more common since 2011.

2022		
Type of Attack	% of Disclosed Breaches	# of Breaches
Unauthorized Access	69%	77
Ransomware	17%	19
Phishing	9%	10
Misconfiguration	5%	6
Malware	3%	3

Unauthorized Access Spotlight

Cybersecurity breaches classified as unauthorized access cover a wide range of attacks with various consequences. For example, in 2022, unauthorized access was attributed to the following breaches:

ALPHA & OMEGA SEMICONDUCTOR Ltd [AOSL] disclosed an incident involving unauthorized access to one company email, which caused the company to make payments to unauthorized bank accounts. This breach caused temporary disruptions and interfered with operations. The company experienced a loss of $ 1.5 million as a result of the incident.

U-Haul Holding Co [UHAL] disclosed a data incident at one of its subsidiaries that allowed attackers to gain access to over two million customer contracts using a compromised contract search tool over a five-month period. As a result, several class action lawsuits relating to the incident have been filed against the company.

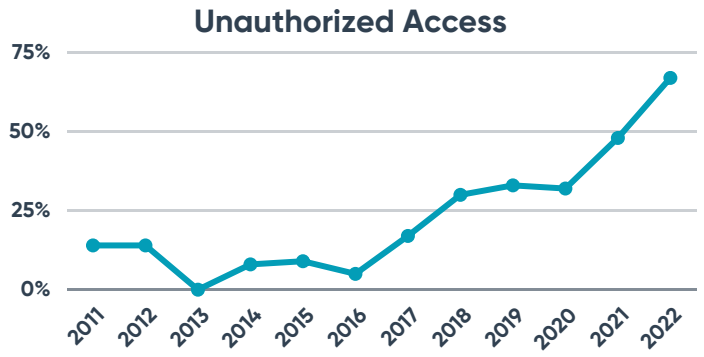
Type of Cybersecurity Attacks

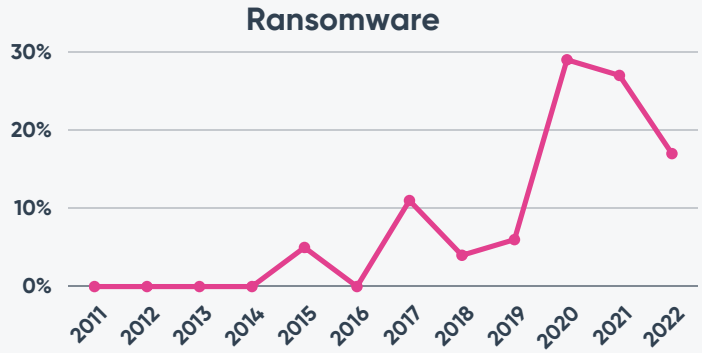
Rank based on percent of total cybersecurity disclosures referencing issue

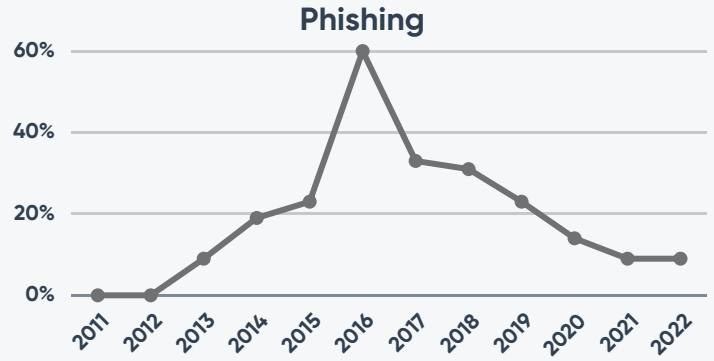
Type of Attack	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Unauthorized Access	14%	14%	0%	8%	9%	5%	17%	30%	33%	32%	48%	69%
Ransomware	0%	0%	0%	0%	5%	0%	11%	4%	6%	30%	27%	17%
Phishing	0%	0%	9%	19%	23%	60%	34%	31%	23%	14%	9%	9%
Misconfiguration	0%	0%	0%	4%	0%	0%	8%	18%	23%	14%	9%	5%
Malware	86%	86%	95%	69%	64%	35%	32%	17%	15%	11%	7%	3%

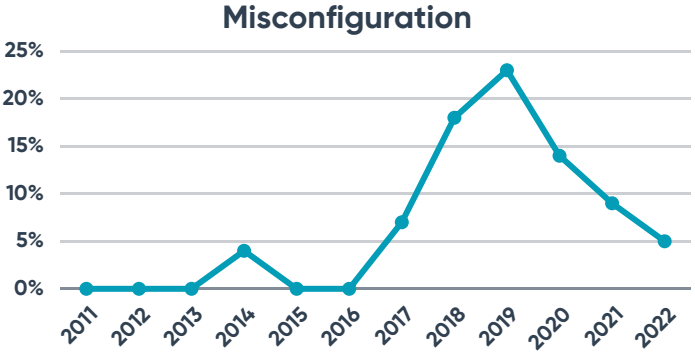
While most types of cybersecurity attacks have begun to trend downward, the percentage of disclosed cybersecurity breaches caused by unauthorized access has been increasing. In each of the last four years, the most common type of incident was unauthorized access breaches.

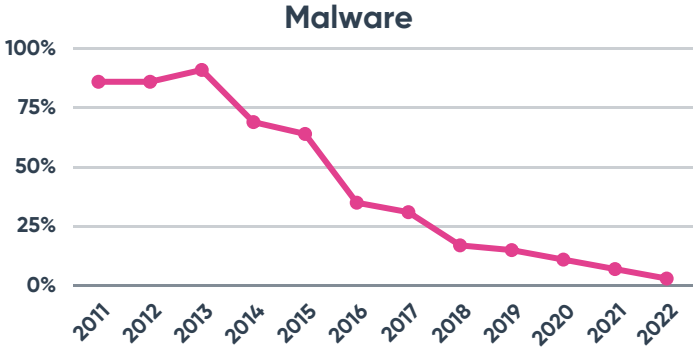
This number skyrocketed in 2022, with unauthorized access contributing to 69% of disclosed breaches during the year, compared to just 48% in 2021 and 32% in 2020.











INFORMATION COMPROMISED

Breaches impacting a company's cybersecurity system can compromise different types of information: personal, financial, or other types of valuable information.

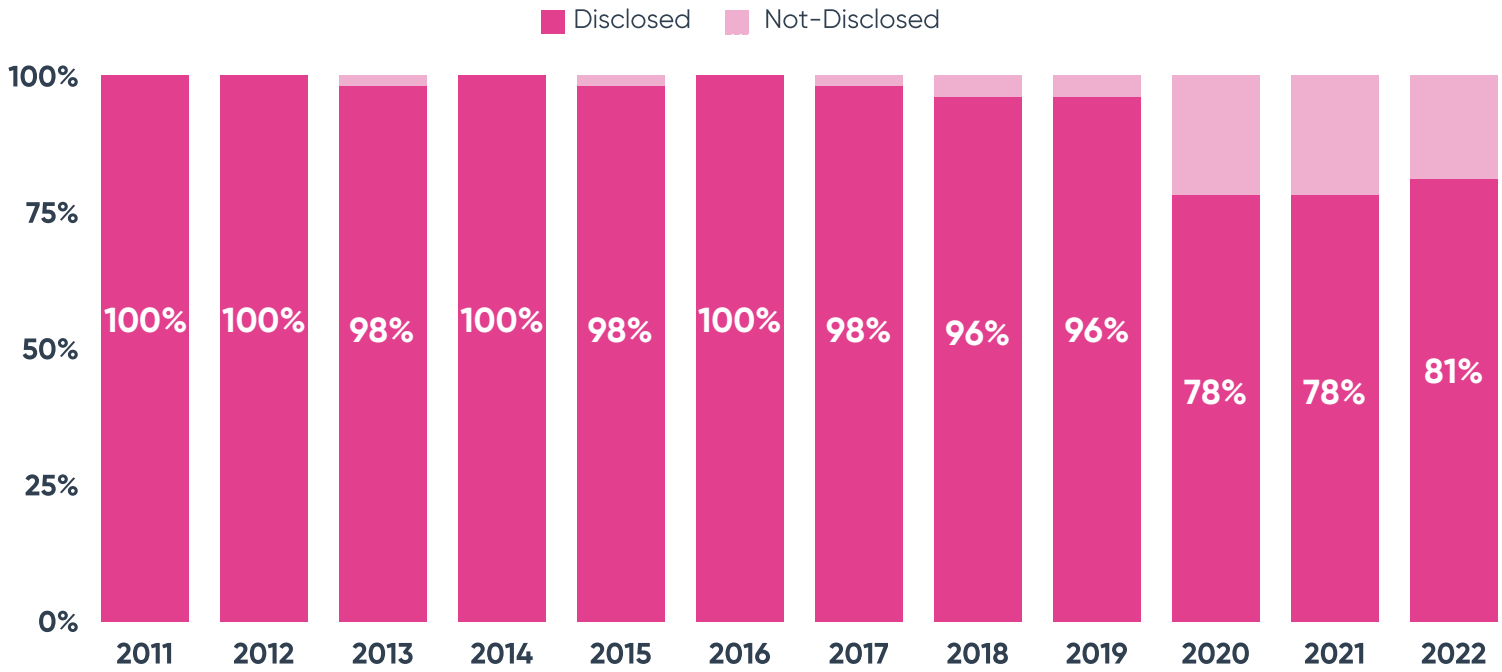
Type of Information	Description
Personal	Name, address, phone number, e-mail, username, password, and SSN.
Financial	Bank accounts, debit and credit cards.
Other	Intellectual property, proprietary business information, and all other types of information.

Although cybersecurity breaches can potentially expose vulnerable company data, it's important to note not every type of attack will result in compromised protected information. For example, in the case of a ransomware attack, this type of breach often seeks to obtain money by holding systems hostage as their primary objective. Under those circumstances, information may not be directly compromised as a result of the attack.

Overall, since 2011, 90% of cybersecurity incident disclosures specified the type of information that was compromised in a cybersecurity breach.

In 2022, 81% of cybersecurity incident disclosures specified the type of information compromised. This is a slight increase from the 78% seen in 2020 and 2021. Prior to 2020, nearly all cybersecurity disclosures specified the type of information compromised.

Information Compromised Disclosed



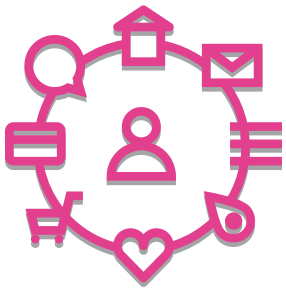
Within a single cybersecurity attack targeting a company's data, the amount of information compromised can vary. In some cases, multiple different types of information are accessed during a breach.

Since 2011, the most common type of information compromised in a cybersecurity breach was personal information, occurring in 78% of all disclosed attacks. Financial data is the least common type of information accessed, seen in only 29% of all disclosed incidents.

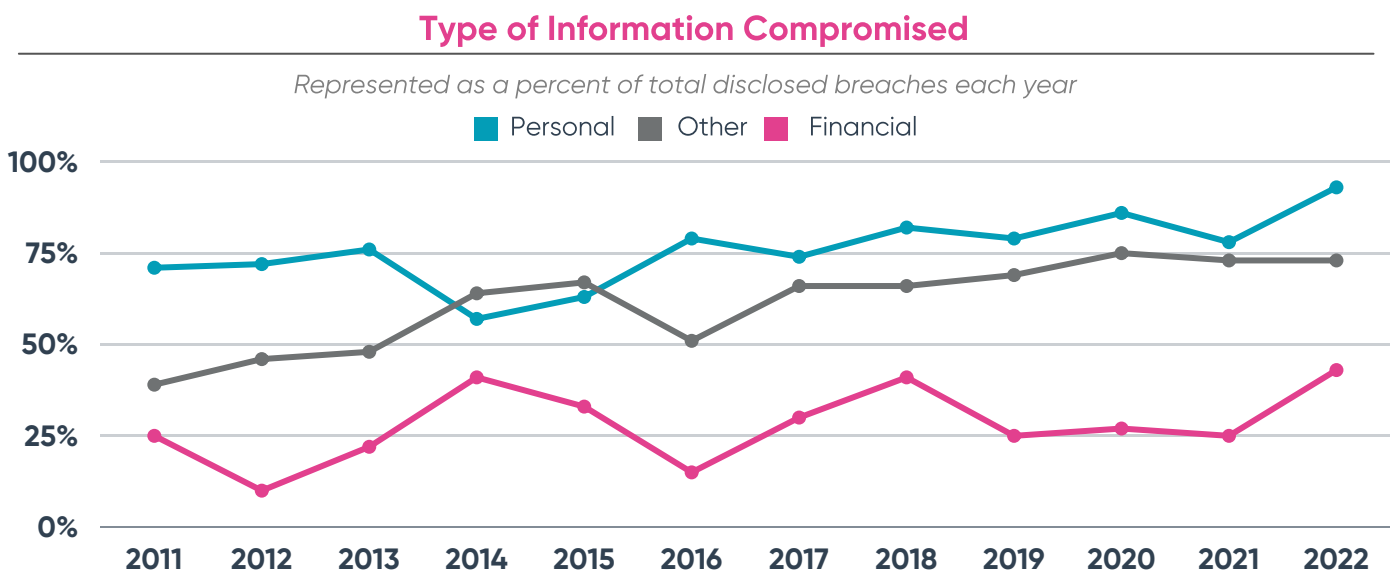
Overall: 2011-2022		
Type of Information	% of Disclosed Breaches	# of Breaches
Personal	78%	781
Other	66%	657
Financial	29%	294

Following the historical trend, the most common type of information compromised in 2022 cybersecurity breaches was personal information, occurring in 93% of disclosed attacks during the year. Financial information was accessed in 43% of disclosed breaches in 2022. In 73% of disclosed cases, other information was accessed.

2022		
Type of Information	% of Disclosed Breaches	# of Breaches
Personal	93%	94
Other	73%	74
Financial	43%	43



The percentage of both personal and financial information accessed in a cybersecurity breach increased in 2022 compared to 2021. Personal information increased 15%, while financial information increased 18%. The proportion of other information accessed remained stagnant in 2022.



Historically, personal names have been the most common type of personal information accessed in disclosed cybersecurity breaches. In 2022, this remained true, with 77% of disclosed breaches specifying that personal names had been accessed as a result of the attack. The second most common type of information compromised was social security numbers, occurring in 62% of disclosed breaches in 2022. The proportion of disclosed breaches that accessed bank account information nearly doubled in 2022, reaching 36%, the highest percentage for banking information seen over the 12-year period.

Information Compromised

represented as a percent of total disclosed breaches each year

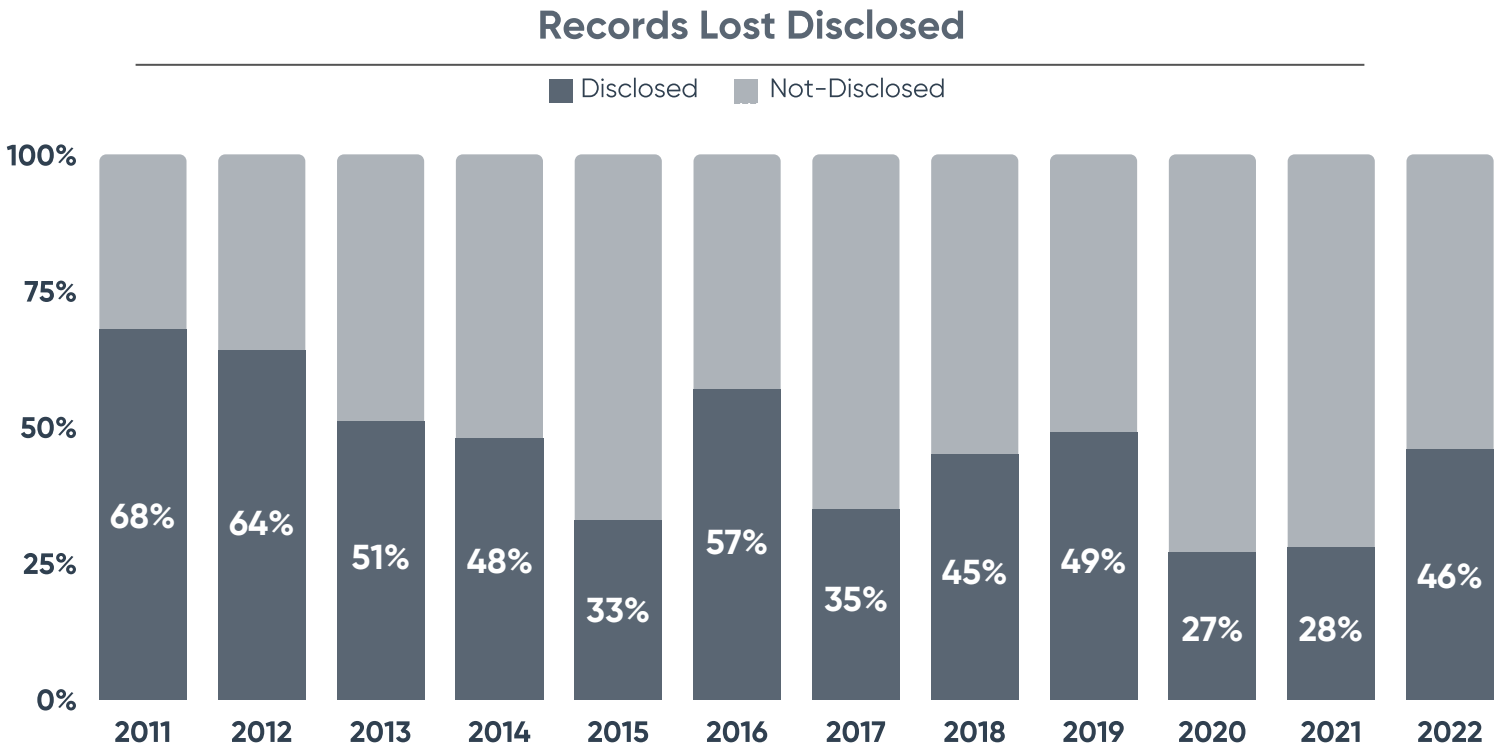
Information Compromised	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Name	64%	49%	63%	44%	50%	56%	57%	65%	61%	68%	65%	77%
SSN	7%	0%	17%	16%	6%	23%	28%	29%	31%	40%	42%	62%
Bank Account	4%	0%	2%	3%	0%	0%	8%	22%	14%	21%	19%	36%
Email	29%	51%	30%	21%	19%	38%	25%	27%	30%	29%	20%	31%
Address	25%	8%	13%	18%	33%	31%	38%	40%	32%	38%	36%	27%
Credit Card	14%	10%	20%	38%	31%	13%	24%	21%	12%	10%	11%	27%
Debit Card	11%	3%	11%	23%	6%	0%	4%	1%	0%	3%	6%	25%
Phone Number	18%	13%	9%	5%	6%	16%	12%	19%	18%	18%	16%	12%
Password	25%	59%	33%	23%	21%	31%	8%	12%	9%	15%	5%	7%
Intellectual Property	4%	10%	2%	11%	10%	2%	5%	2%	0%	3%	4%	4%
User name	32%	31%	37%	13%	13%	13%	2%	7%	7%	13%	3%	3%

2022 Information Compromised Trends

Type of Information	Percentage Point Increases from 2021
SSN	20
Debit Card	19
Bank Account	17
Credit Card	16
Name	12
Email	10
Other	2
Password	2

Type of Information	Percentage Point Decreases from 2021
Address	-9
Phone Number	-4

RECORDS LOST



Similar to information compromised, a cybersecurity attack does not always result in a number of records stolen. Moreover, the number of lost records is also not required to be disclosed. Overall, since 2011, 41% of cybersecurity incident disclosures specified the number of records lost during an attack.

In 2022, 46% of cybersecurity incident disclosures specified the number of records lost as a result of a cybersecurity incident. This is the largest percentage of disclosed records lost since 2019.

Overall: 2011-2022 Average Records Lost

Attack	Average Records Lost
Misconfiguration	66,238,378
Malware	20,468,388
Unauthorized Access	9,664,781
Phishing	1,502,646
Ransomware	648,308

Overall, misconfiguration cybersecurity attacks resulted in the highest average number of disclosed records lost at over 66 million records per breach. A distant second, averaging nearly 20.5 million in lost records, are malware breaches. Ransomware is the least vulnerable type of breach overall in terms of lost records, averaging less than one million records per disclosed breach.

Altaba Inc., previously Yahoo Inc. at the time of the breach, recorded the largest number of records lost over the 12-year period as the result of a cybersecurity breach. The company lost three billion records in a cyber-attack disclosed in 2016.

Three out of the top five breaches in terms of lost records resulted from misconfiguration attacks. CVS was informed of a misconfiguration breach in March 2021 resulting from the exploitation of a non-password protected database that contained over one billion records managed by a CVS Health vendor. The breach was discovered by an outsourced cybersecurity research team.

Top 5 Most Records Lost: 2011 - 2022

Rank	Company	Disclosure Year	Records Lost (in millions)	Types of Breach	Information Accessed
1	Altaba	2016	3,000	Not disclosed	Email | Name | Other | Password | Phone Number
2	Baidu	2017	2,000	Not disclosed	Name | Other
3	CVS	2021	1,000	Misconfiguration	Email | Other
4	First American Financial Corp	2019	885	Misconfiguration	Bank Account | Other | SSN
5	Meta Platforms	2019	540	Misconfiguration	Name | Other

In 2022, there were only 56 cybersecurity breaches that provided the number of records lost as a result of the attack. Of the disclosed breaches, only five companies reported over one million lost records.

Twitter, Inc. disclosed the highest number of lost records in 2022, exceeding five million as a result of a misconfiguration attack. In one instance, a threat actor was able to exploit a bug in the system and access personal information connected to celebrities, companies, and common users' accounts globally. That information was later advertised for sale for $30,000.

2022 Cybersecurity Breaches: Over 1 Million Records Lost

Rank	Company	Disclosure Date	Records Lost (in millions)	Types of Breach	Information Accessed
1	Twitter	8/5/2022	5.4	Misconfiguration	Email | Other | Phone Number
2	Nelnet	8/26/2022	2.5	Unauthorized Access	Address | Email | Name | Phone Number | SSN
3	Walgreens Boots Alliance	7/22/2022	2.4	Unauthorized Access	Name | Other | SSN
4	U-Haul Holding Co.	9/9/2022	2.2	Unauthorized Access	Name | Other
5	Flagstar Bancorp	6/14/2022	1.5	Unauthorized Access	Address | Bank Account | Name | Other | SSN

CYBERSECURITY BREACH TIMEFRAME

An analysis on the cybersecurity breach timeframe reviewing the average and median number of days within the breach discovery and disclosure windows.

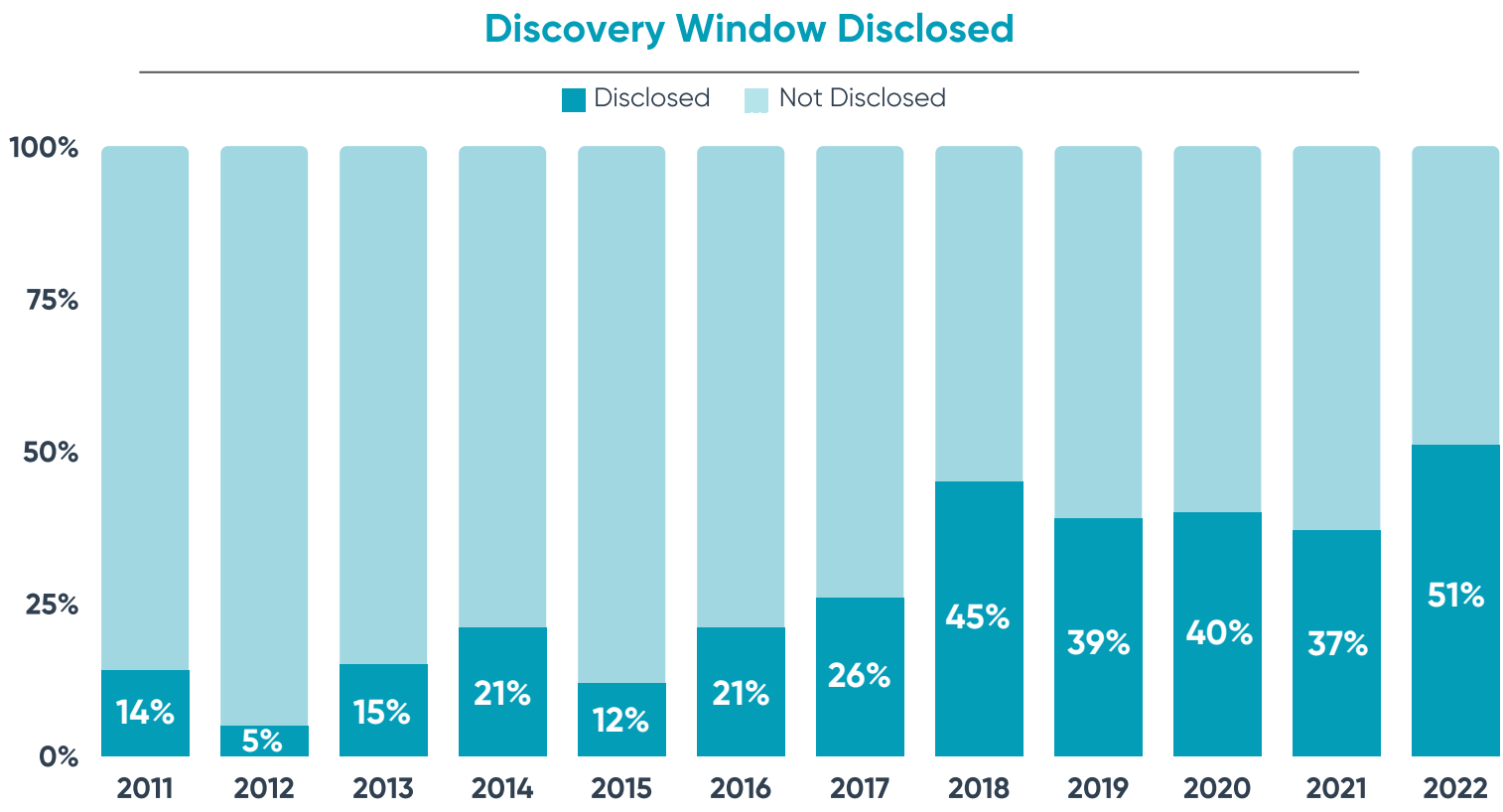
Date	Description
Breach Start	The date the cybersecurity attack first began, if able to be determined
Breach Discovery	The date disclosed by the company on which they first discovered the breach.
Breach Disclosure	The first date in which the breach became publicly known by a company, news report, or cybersecurity blog announcement as well as the date a breach is reported on a state Attorney General's website.

There are three key dates that relate to a cybersecurity attack on a public company: when it began, when it was discovered, and when it was publicly disclosed.

The timeframe between when a cybersecurity breach began, if able to be determined, and when the breach was discovered constitutes the 'discovery window'. Long discovery windows raise red flags about internal controls, as insufficient cybersecurity controls can inhibit the timely detection of issues.

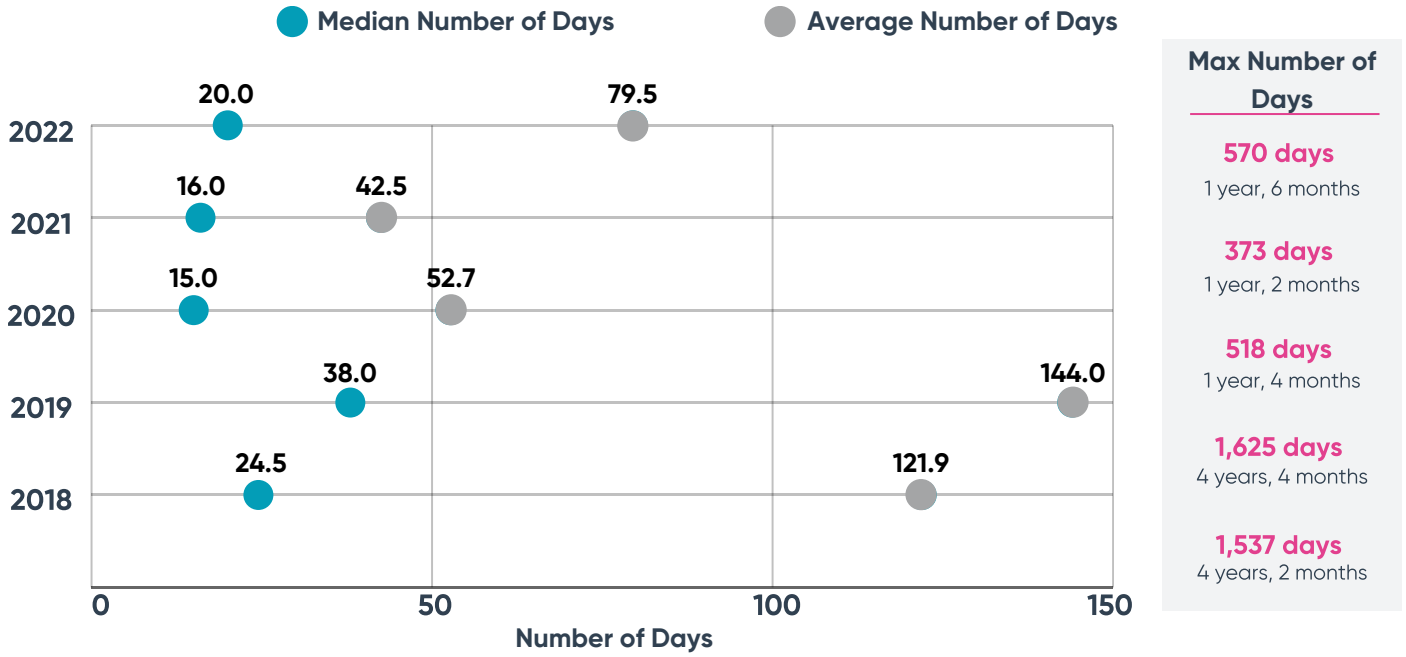
Overall, since 2011, 34% of cybersecurity incident disclosures specified both the date that the breach began and the date the breach was discovered.

In 2022, 51% of breaches disclosed both the date of the attack and the date of discovery. This is the largest percentage of breach disclosures that specified the discovery window over the 12-year period. Before 2022, less than half of breach disclosures provided this information.



DISCOVERY WINDOW

Breach Discovery Window Timeframe



Over the last five years, the average number of days it took for companies to discover a breach after it began was 86.3 days; the median was 22 days.

In 2022, on average, it took 79.5 days for companies to discover a breach, with a median of 20 days. This represented an 87% increase in the average discovery window from 2021 and a 25% increase in the median.

The longest discovery window in 2022 was 570 days, indicating it took over a year and a half for the company to discover the breach. The cybersecurity breach was an unauthorized access attack on Transunion, a credit reporting agency, that began in January 2021 and was not discovered until July 2022. In comparison, Golden Entertainment (a casino, tavern, and gaming hub) saw the longest discovery window in 2021 of 373 days to discover a malware attack on their systems.

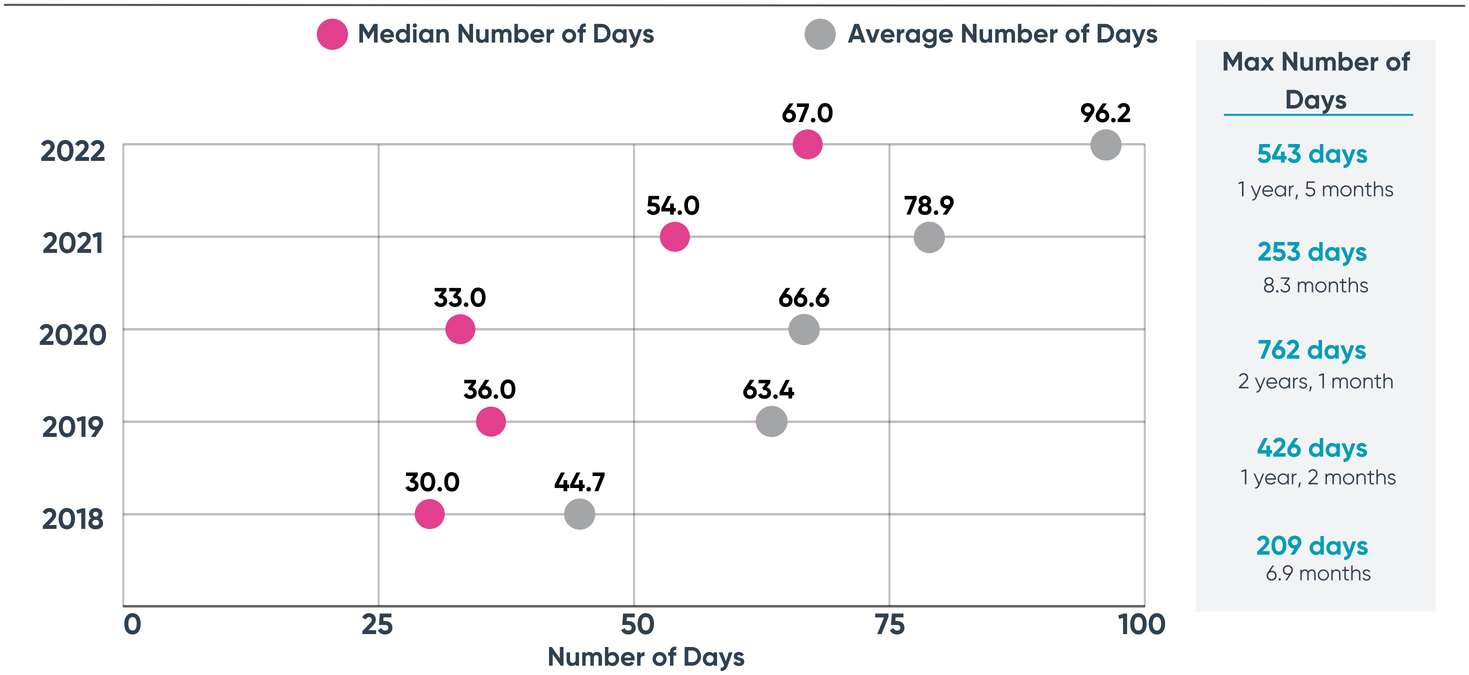
DISCLOSURE WINDOW

The disclosure window is considered to be the timeframe between when a breach was discovered and when it was first publicly disclosed. Though there are no standard regulatory requirements for disclosure dates, the SEC provides guidance to "consider the materiality of cybersecurity risks and incidents when preparing the disclosure."[3] If a cybersecurity breach is expected to have material impacts, it must be disclosed within four days in a current report with the Commission (8-K filing).

Furthermore, requirements for breach disclosures vary widely from state to state. Many states require cybersecurity breaches to be disclosed "without unreasonable delay", resulting in varying disclosure windows.

Failure to disclose a cyber breach in a timely manner after discovery could have serious repercussions, including SEC fines and negative market reaction from investors, especially if the breach is disclosed by a third party and not the affected party itself.[4] For consumers impacted by a data breach, a lag in disclosure time diminishes their ability to quickly react and inhibits timely protection and detection efforts to mitigate potential threats to their information, such as credit monitoring.

Breach Disclosure Window Timeframe



Over the last five years, the average number of days it took for companies to disclose a breach after it had been discovered was 70.8 days, with a median of 40.5 days.

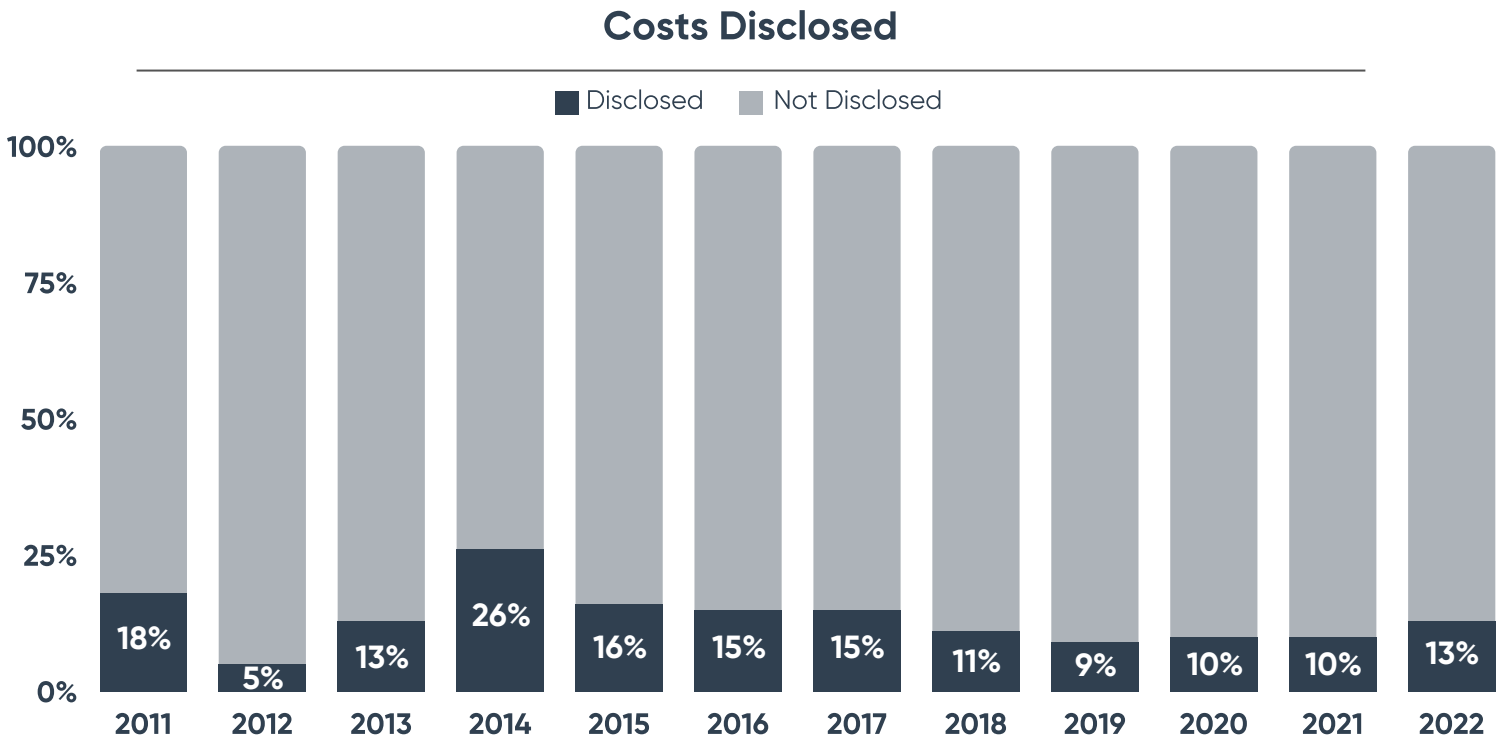
In 2022, on average, it took 96.2 days to disclose a breach after being discovered and a median of 67 days. The longest average and median disclosure windows of the last five years were seen in 2022.

The longest disclosure window in 2022 lasted 543 days, nearly 18 months. Hertz Global Holdings discovered an unauthorized access breach of a subsidiary in March 2021 and did not disclose the incident until August 2022. In comparison, the longest disclosure window in 2021 was 253 days, about eight months.

3 Securities and Exchange Commission. CF Disclosure Guidance: Topic No. 2 – Cybersecurity (October 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
4 Amir, Eli and Levi, Shai and Livne, Tsafrir. Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets (June 7, 2018). Review of Accounting Studies, available at https://ssrn.com/abstract=3136193.

CYBERSECURITY COSTS

Depending on the severity of the attack, cybersecurity breaches can result in a litany of costs. Investigation, remediation, and legal fee costs are a few examples of a direct financial impact imposed by a breach. The risk of economic and reputational costs can also directly impact the financial performance of a company, such as reduced revenue due to lost sales. In extreme cases, such costs can potentially have a further material adverse impact on a company's business.

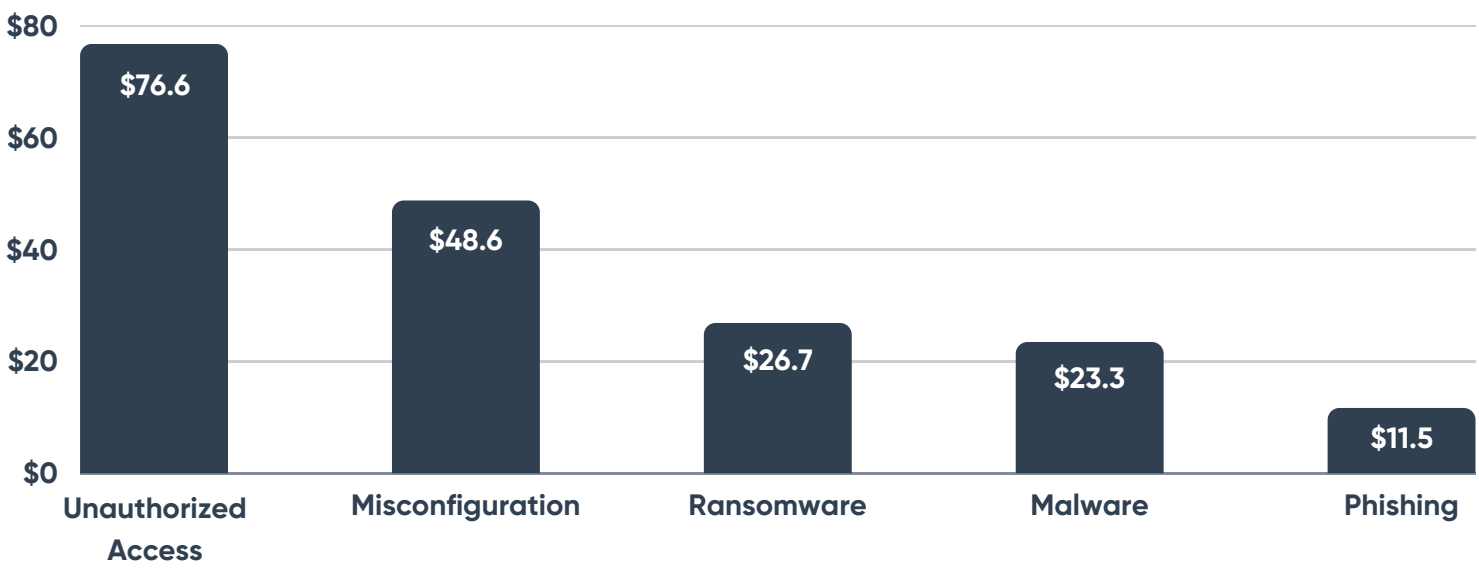


Overall, since 2011, 12% of cybersecurity incidents disclosed specified costs associated with the breach.

In 2022, 13% of breaches disclosed specific costs due to a cybersecurity incident. The low rates in material cost disclosures may be due to the fact that exact costs may not be readily available after a breach, and subsequent filings can add more details after a thorough assessment. Additionally, some cybersecurity breaches may not incur any material costs as a result of the breach.

Disclosed records only include those that reported a specific cost amount incurred due to the attack. The static trend in the percentage of breaches that disclose costs may be attributed to limited information about newer incidents.

Average Cost by Type of Breach



Since 2011, unauthorized access cybersecurity attacks have resulted in the highest average costs, averaging $76.6 million per breach. Misconfiguration attacks rank second, averaging $48.6 million in disclosed costs. Phishing is the least costly type of breach overall, averaging $11.5 million in disclosed costs per attack.

Similarly, unauthorized access cybersecurity attacks have the highest overall disclosed costs, totaling $10.4 billion since 2011. All other categories of cybersecurity breaches – malware, ransomware, phishing, and misconfiguration – have total disclosed costs of less than $1 billion each.

Three of the top five costliest breaches since 2011 resulted from unauthorized access attacks. The unauthorized access breaches that impacted Meta Platforms (formerly known as Facebook) in 2018 and Equifax in 2017 cost the companies each over $1 billion.

Top 5 Costliest Breaches: 2011 - 2022

Rank	Company	Disclosure Year	Total Costs (in millions)	Types of Breach	Information Accessed
1	Meta Platforms	2018	$5,100	Unauthorized Access	Not disclosed
2	EQUIFAX	2017	$1,703	Unauthorized Access	Address | Credit Card | Name | Other | SSN
3	Natura & Co Holding	2020	$454	Not Disclosed	Not disclosed
4	Merck & Co.	2017	$380	Ransomware	Not disclosed
5	HOME DEPOT	2014	$298	Unauthorized Access	Pay Cards

In 2022, there were only 16 disclosed cybersecurity breaches that provided specified costs as a result of the attack. This lack of disclosure is not unusual, as costs may not be fully realized at the time of the attack, or the breach may not directly result in material financial harm.

Expeditors International of Washington incurred a total of $60 million in disclosed costs as a result of a cybersecurity attack in February 2022. The company was forced to temporarily limit operations for three weeks to contain and eliminate the cybersecurity threat. As a result, the company incurred $40 million in demurrage charges for its inability to complete shipments in a timely manner. Additionally, the company spent $20 million on cybersecurity consulting services to recover its systems and enhance cybersecurity protections.

2022 Cybersecurity Breaches: Costs Exceeding $1 million

Rank	Company	Disclosure Date	Total Costs (in millions)	Types of Breach	Information Accessed
1	Expeditors International of Washington	2/20/2022	$60.0	Not Disclosed	Not disclosed
2	Hanesbrands	5/31/2022	$15.5	Ransomware	Address | Bank Account | PayCards | Name | Other | Phone Number | SSN
3	Ardagh Metal Packaging	7/15/2022	$15.0	Ransomware	Bank Account | Name | Other | SSN
4	Progress Software	12/19/2022	$4.8	Unauthorized Access	Not disclosed
5	Exela Technologies	8/10/2022	$3.7	Not Disclosed	Not disclosed
6	Alpha & Omega Semiconductor	5/10/2022	$1.5	Unauthorized Access	Email
7	Omnicell	8/4/2022	$1.4	Ransomware	Bank Account | Pay Cards | Other | SSN
8	Montrose Environmental Group	6/14/2022	$1.0	Ransomware	Bank Account | Pay Cards | Name | Other

DATABASE OVERVIEW AND METHODOLOGY

OVERVIEW

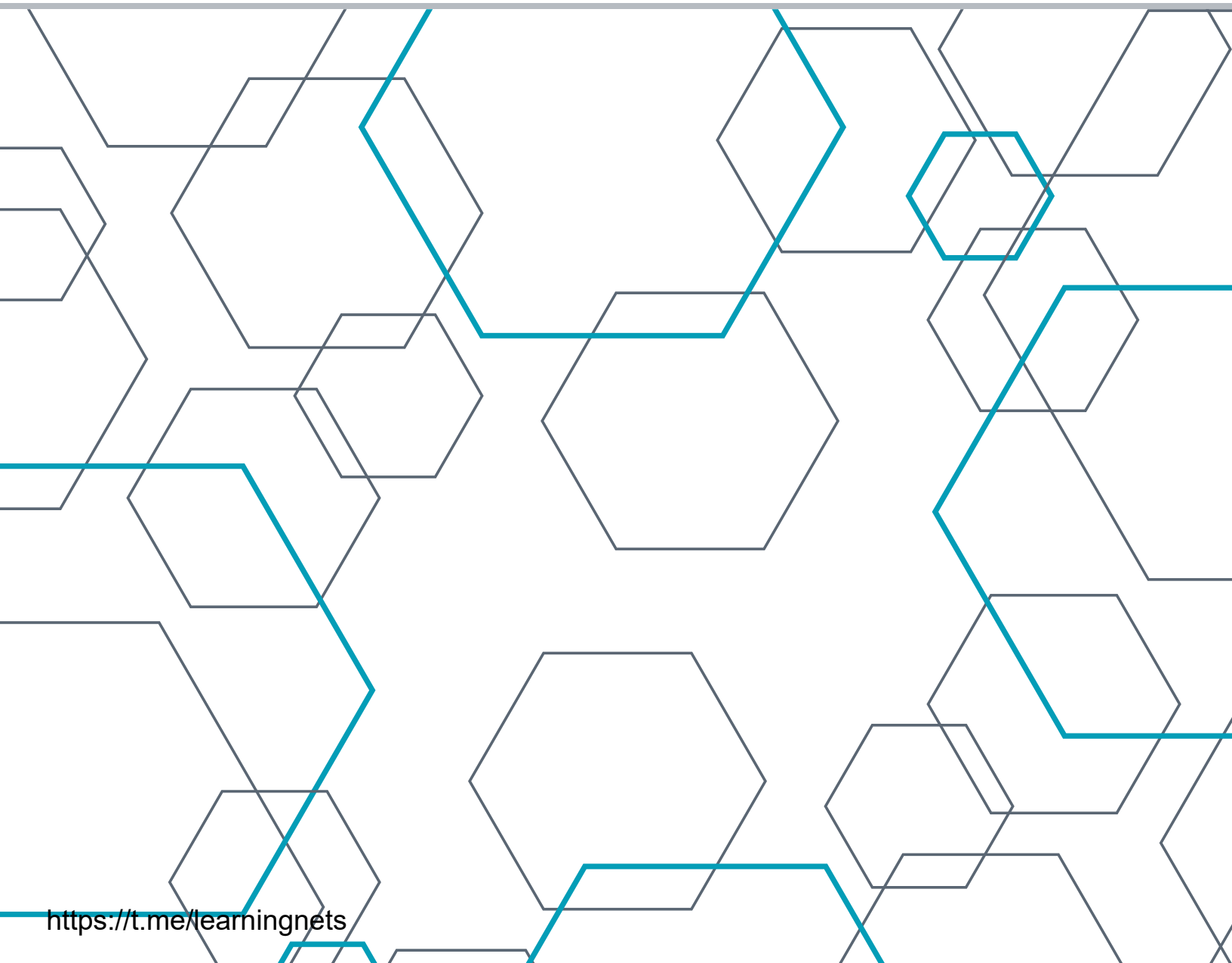
The Audit Analytics Cybersecurity database can be used to track the disclosure of and impacts arising from cybersecurity data breaches affecting public companies. This database makes it easy to locate the earliest public disclosure and provides updated details related to the breach on an ongoing basis, as the information becomes available.

Data covers SEC registrants (foreign and domestic) since 2010. Data is updated daily and can be accessed through the Audit Analytics website and data feeds.

METHODOLOGY

This report covers publicly disclosed cybersecurity breaches by SEC registrants. Disclosure dates based on year of first disclosure, from 2011 to 2022.

Sources for the disclosures include: SEC filings, state documents, and press coverage. Breach records are periodically updated with further details, if and when disclosed.



AUTHORS

Kayla Coello-Aude — *Research Analyst*
Sarah Keohane — *Data Analyst*
Marie Pupecki, CPA — *Senior Accounting Research Analyst*

ABOUT US

Whether for market intelligence, risk management, compliance, or research and public policy, Ideagen Audit Analytics provides the highly structured data you need to make informed decisions.

Our expert team meticulously collects, organizes, and analyzes data – making it easy for our customers find what they need to know. We are trusted to simplify the complex; to illuminate trends; and to reveal actionable insights.

CONTACT US

Ideagen Audit Analytics

North America
13450 W. Sunrise Blvd., Suite 160
Sunrise, Florida 33323

Phone: 508.476.7007
Email: info@auditanalytics.com