AUDIT ANALYTICS®

an Ideagen solution

# TRENDS IN CYBERSECURITY BREACH DISCLOSURES

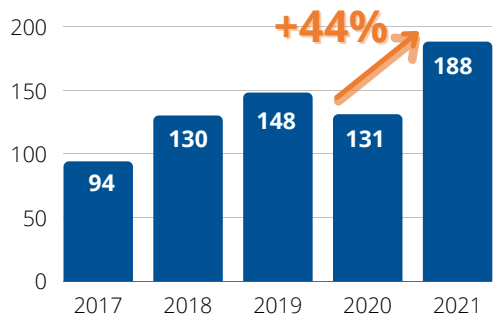
APRIL 2022

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

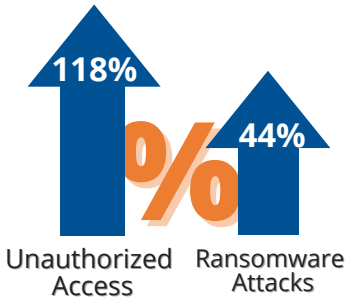
## 1 44% increase in the number of cybersecurity breaches disclosed in 2021.

In 2021, 188 breaches were disclosed by public companies. This is the most breaches disclosed in a single year since 2011.



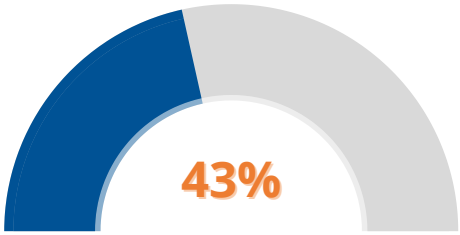

## 2 Increase in unauthorized access breaches and ransomware attacks between 2020 and 2021.

Cybersecurity breaches related to unauthorized access increased 118%. Ransomware attacks increased 44%.




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

In 2021, 43% of cybersecurity incidents were disclosed in a filing with the SEC. Most commonly, the disclosure appeared in the Risk Factors section of a periodic report.




## 4 On average, companies took 80 days to disclose a breach after it was discovered.

In 2021, companies averaged 79.8 days to disclose a breach after it occurred. In 2020, the average disclosure window was 60.6 days, almost 3 weeks shorter.

# INTRODUCTION

As the digital age of information and technology has rapidly integrated into daily life, the importance of cybersecurity has become paramount for businesses. There has been an explosion in the amount of data transmitted digitally and an increased reliance on technology.

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

How, when, and what businesses must disclose following a breach varies depending on the entity requiring the 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.** What type of attack occurred that allowed an incursion into company systems?
  i.e. Malware, unauthorized access, phishing.
- **Information compromised.** What or whose information was compromised?
  i.e. Personal or financial information belonging to employees or consumers, intellectual property.
- **Timeframe.** When did the breach happen, when was it discovered, and when was it disclosed?
  i.e. A long-term, unknown intrusion into systems vs. a one-time attack discovered immediately.
- **Costs.** What, if any, costs were incurred by the company associated with the incident?
  i.e. Remediation costs, the need to engage cybersecurity experts, litigation.

The SEC disclosure requirements currently under Regulation S-K and Regulation S-X do not currently refer specifically to cybersecurity events. However, 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]

The disclosure requirements for cybersecurity incidents are undergoing a shift in focus to enhancing and standardizing disclosures for cybersecurity governance, strategy, and risk management. As of March 2022, the SEC is considering proposed amendments to its rules regarding the cybersecurity disclosures of public companies.[2] These proposed rules include a host of provisions, such as:

- 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 regards to cybersecurity risks; and management's role and expertise with cybersecurity matters;
- Cybersecurity disclosures must be made using inline XBRL.

Presenting information about cybersecurity risks and incidents in a consistent, comparable, and decision-useful manner would benefit both companies and investors.

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 (March 9, 2022). SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2022-39

# TRENDS IN DISCLOSURES

## Overview

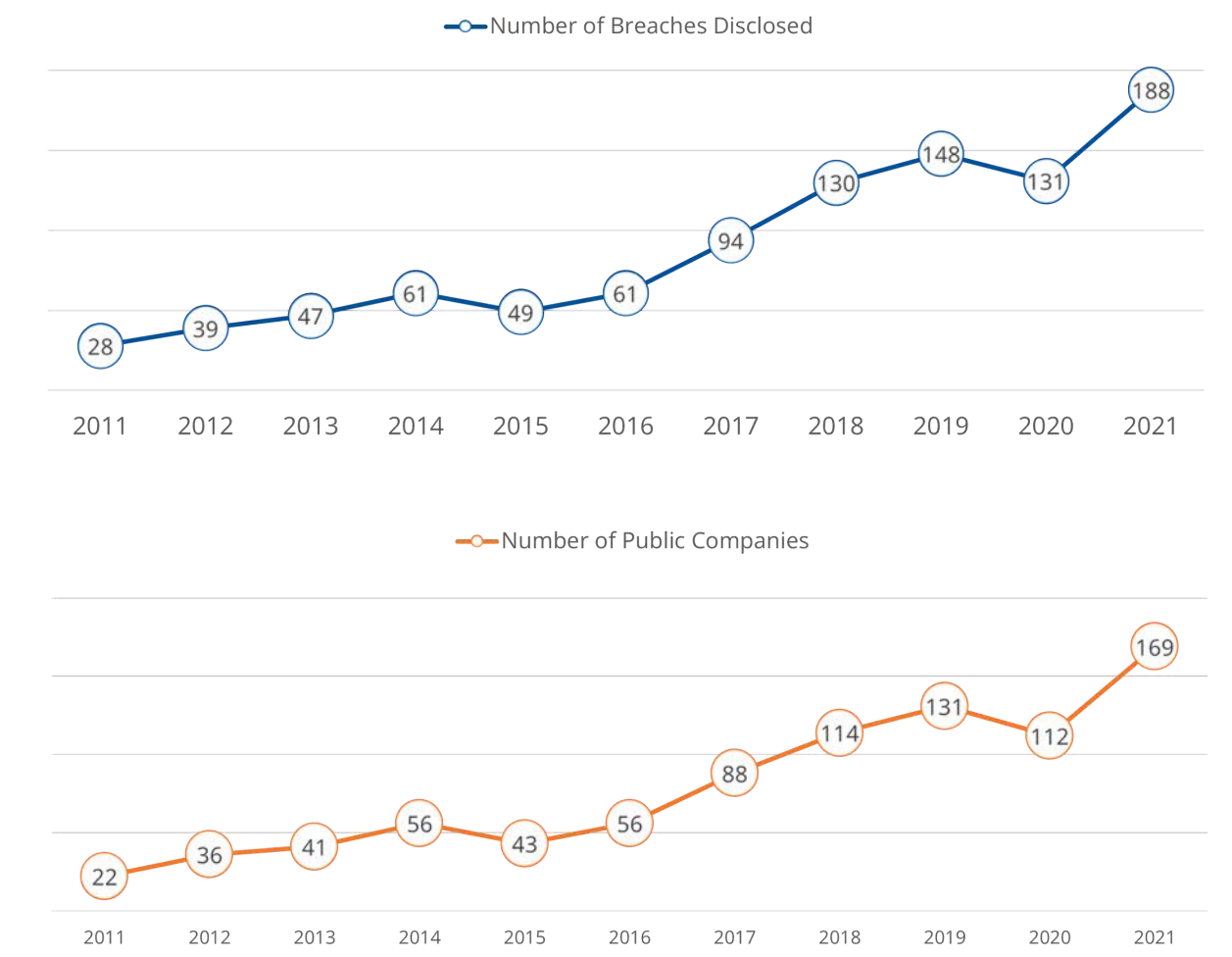
The number of cybersecurity incidents disclosed during the calendar year 2021 reached a record high of 188 incidents reported by 169 unique public companies.

Between 2020 and 2021, the number of cybersecurity incidents increased by 43.5%. The number of companies impacted by cybersecurity incidents rose 50.9%.

Since 2011, the number of disclosed cybersecurity incidents annually has increased nearly 600%. The prevalence of cybersecurity incidents started sharply rising after 2016. Slight decreases year-over-year were noted in both 2015 and 2020.

The number of breaches is higher than the number of companies disclosing the incident because companies can be victimized more than once.

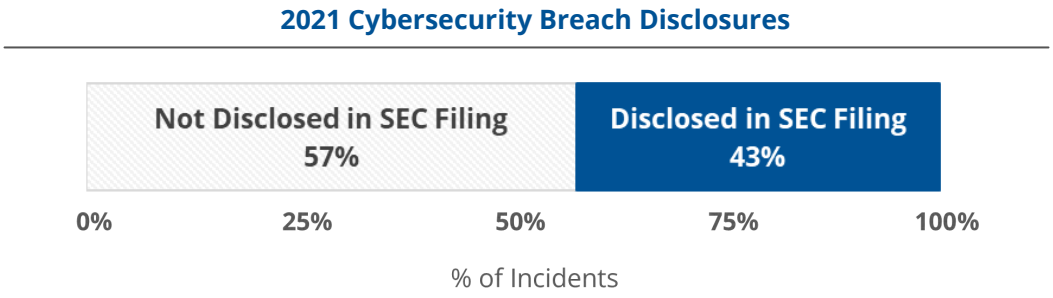
### Cybersecurity Breach Disclosures



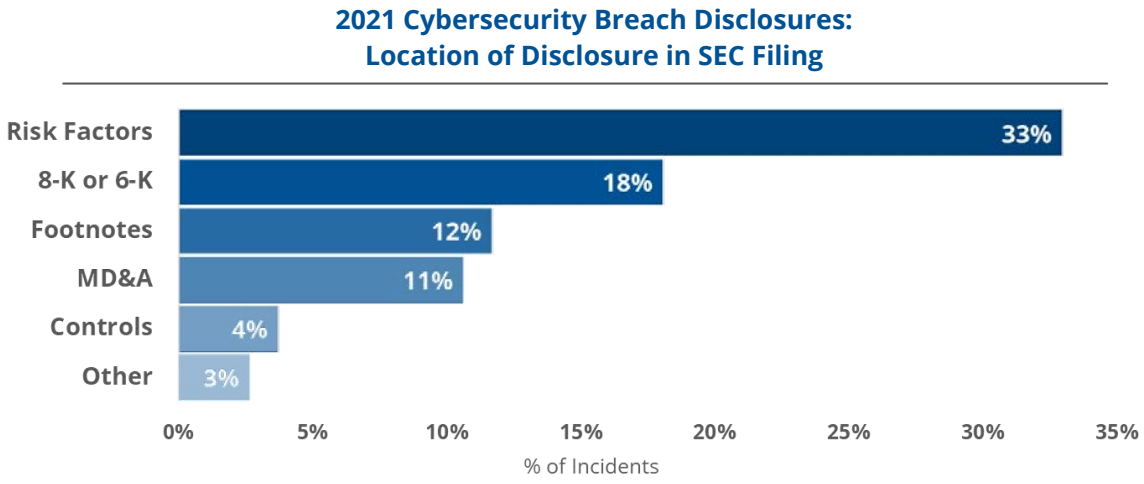
## Method of Disclosure

As mentioned in the Introduction, there is no general requirement for public companies to disclose cybersecurity incidents in a filing with the SEC, though there are certain provisions where disclosure is required. Cybersecurity incident disclosure sources outside the SEC include press coverage and notifications from state attorney generals' offices.

Of the 188 cybersecurity incidents that were disclosed in 2021, 43% were discussed in a filing with the SEC. This includes either the first disclosure of the incident or any further details provided by the company thereafter.




By far, the most common location in an SEC filing for a company to discuss a cybersecurity breach in 2021 was as a risk factor, encompassing 33% of breaches. 18% were disclosed in a current report, either Form 8-K or 6-K. 12% of 2021's cybersecurity incidents that were discussed in SEC filings were disclosed in the footnotes to financial statements, and 11% were disclosed in the management's discussion and analysis (MD&A). Only 4% discussed the cybersecurity breach concerning a company's controls. 3% of breaches were disclosed elsewhere in an SEC report.



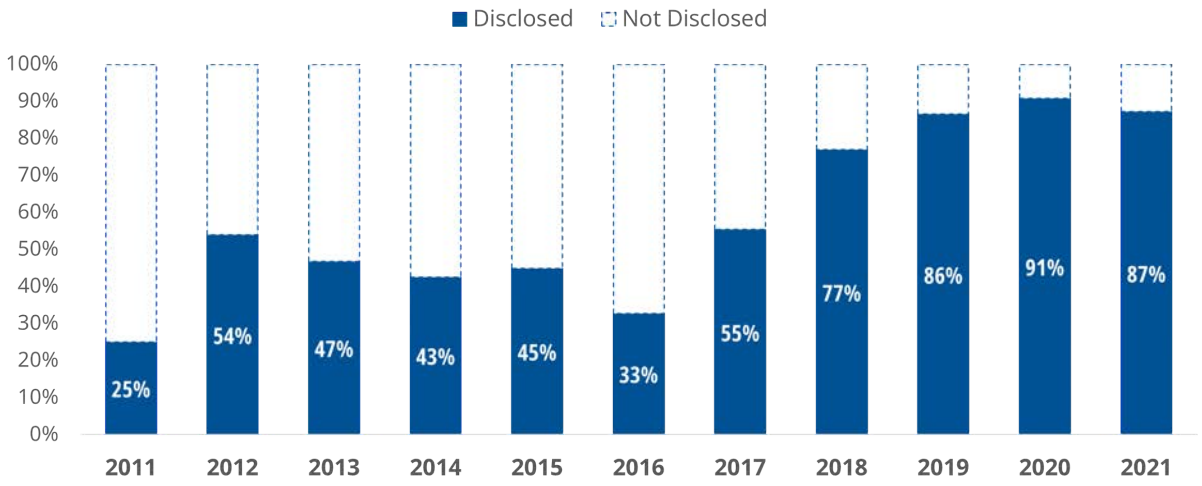

A cybersecurity incident is notable in terms of a company's controls. In October 2018, the SEC issued an investigative report advising companies to consider and assess the potential impact of cyber threats when implementing internal accounting controls.[3] SOX 302 requires companies to disclose all changes that could materially affect internal controls over financial reporting (ICFR), including remediation of ICFR deficiencies related to cybersecurity and any changes that were made to improve controls following a breach. If controls are insufficient to prevent a cybersecurity attack, material changes made to remediate the deficiency would be a required disclosure.

3 Securities and Exchange Commission (October 16, 2018). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements. https://www.sec.gov/litigation/investreport/34-84429.pdf

## Types of Attack

Overall, since 2011, 70% of cybersecurity incident disclosures specified the type of attack used to penetrate the company's systems.

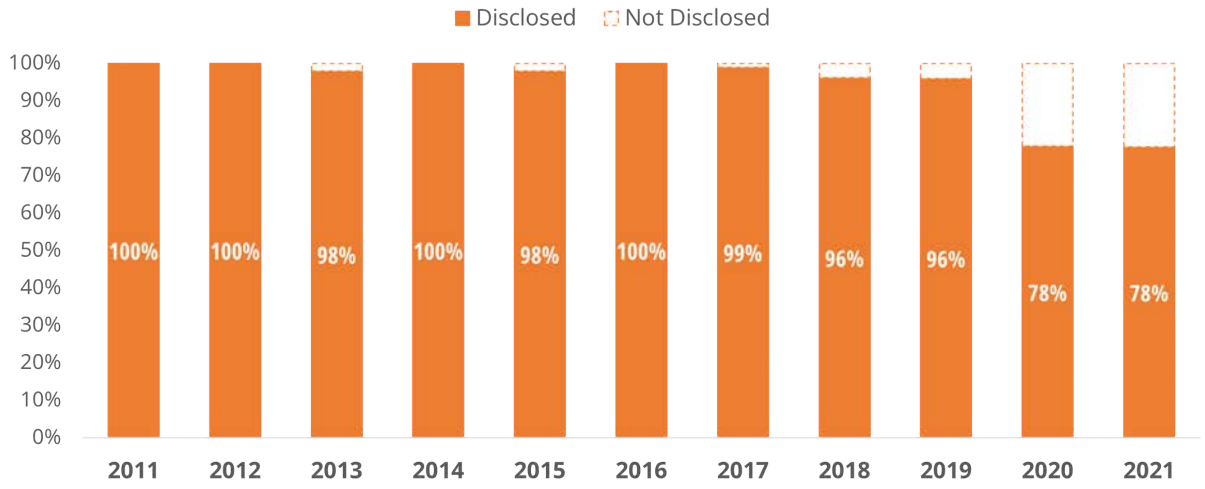
In 2021, 87.2% of cybersecurity incident disclosures specified the type of attack used. Since 2016, there has been an upward trend in disclosing the type of attack. At the low point in 2011, only 25.0% of disclosures disclosed the type of attack.




## Information Compromised

Overall, since 2011, 91.3% of cybersecurity incident disclosures specified the type of information compromised in a cybersecurity breach.

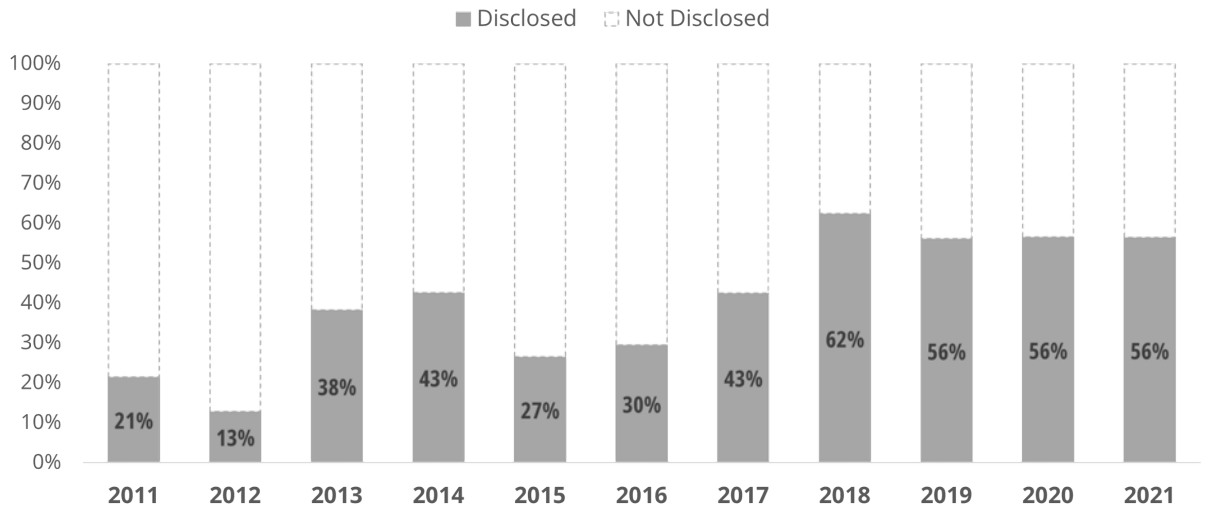
In 2021, 77.7% of cybersecurity incident disclosures specified the type of information compromised. This is a slight decrease from the previous low point of 77.9% in 2020. In 2011, 2012, 2014, and 2016, 100% of disclosures specified the type of information compromised.



## Discovery

Overall, since 2011, 48.2% of cybersecurity incident disclosures specified the date that the breach was discovered.

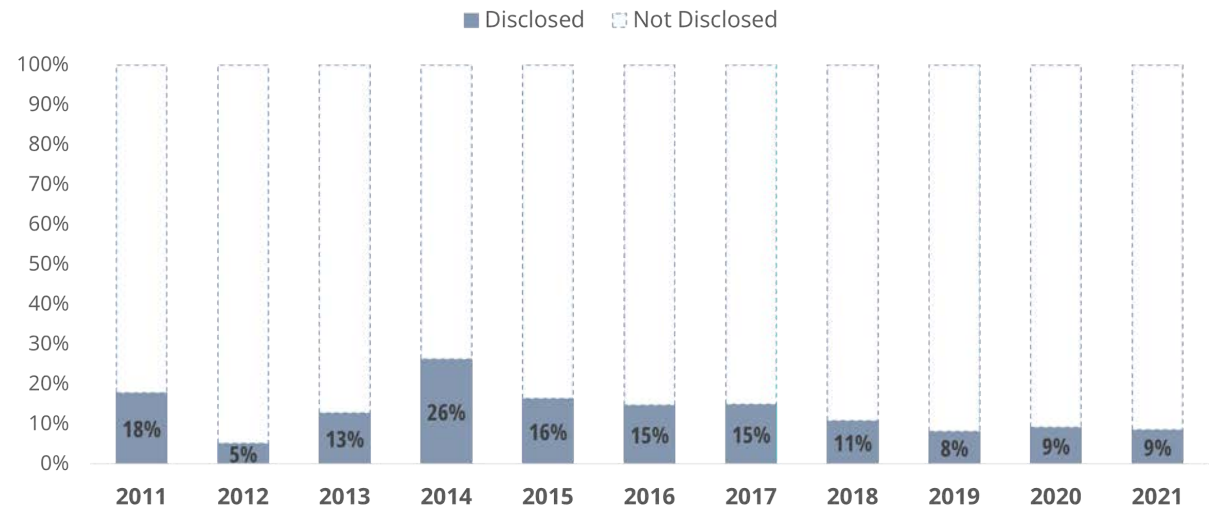
In 2021, 56.4% of breaches disclosed the date that the breach was discovered. Before 2018, less than 50% of breach disclosures each year disclosed the date that the breach was discovered. In comparison, at the low point in 2012, 12.8% disclosed the date of the breach. At the high point in 2018, 62.3% disclosed the date the breach was discovered.




## Costs

Overall, since 2011, 11.2% of cybersecurity incidents disclosed specified costs associated with the breach.

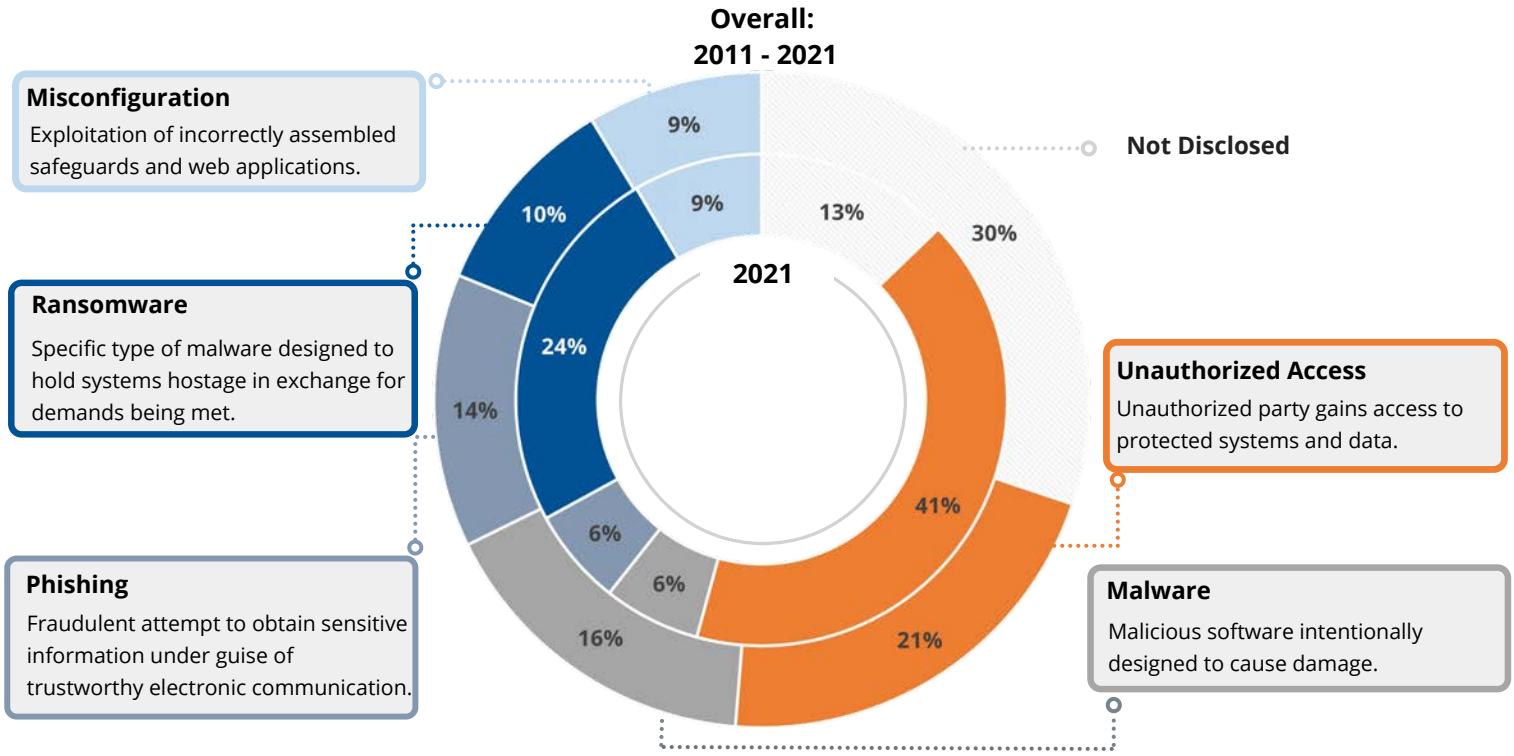
In 2021, 8.5% of breaches disclosed specific costs associated with the incident. Exact costs may not be readily available after a breach and subsequent filings can add more details after a thorough assessment. Therefore, the downward trend in the percent of breaches that disclose costs can partially be attributed to less information about newer incidents.



# TRENDS IN CYBERSECURITY INCIDENTS

## Types of Attacks

Breaches impacting a company's cybersecurity breaches can be attributed to different types of attacks: malware, ransomware, phishing, unauthorized access, and misconfiguration.

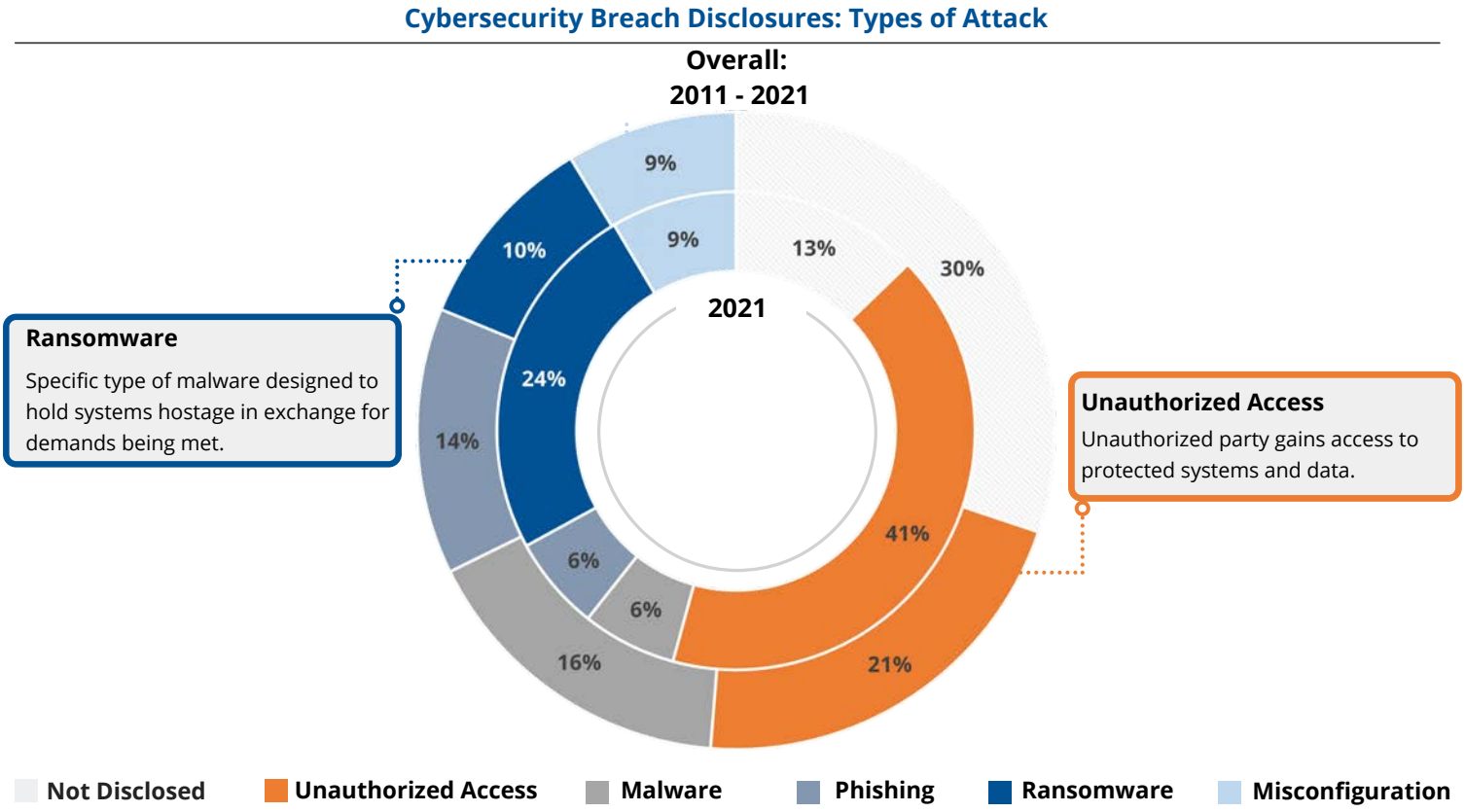



Since 2011, the most common type of cybersecurity breaches are related to unauthorized access, contributing to 21.2% of total disclosed attacks. The second most common type of breach since 2011 is malware incidents, contributing to 16.5% of total disclosed attacks. The third most common is phishing, contributing to 13.5% of breaches, followed by ransomware and misconfiguration.

In 2021, in line with the overall trend, the most common type of cybersecurity breaches related to unauthorized access, contributing to 41.5% of total disclosed attacks. Ransomware attacks in 2021 were the second most common type of cybersecurity incident, contributing to 24.5% of breaches disclosed during the year. This is significantly higher than the overall trend; ransomware is only the fourth most common attack type disclosed since 2011.

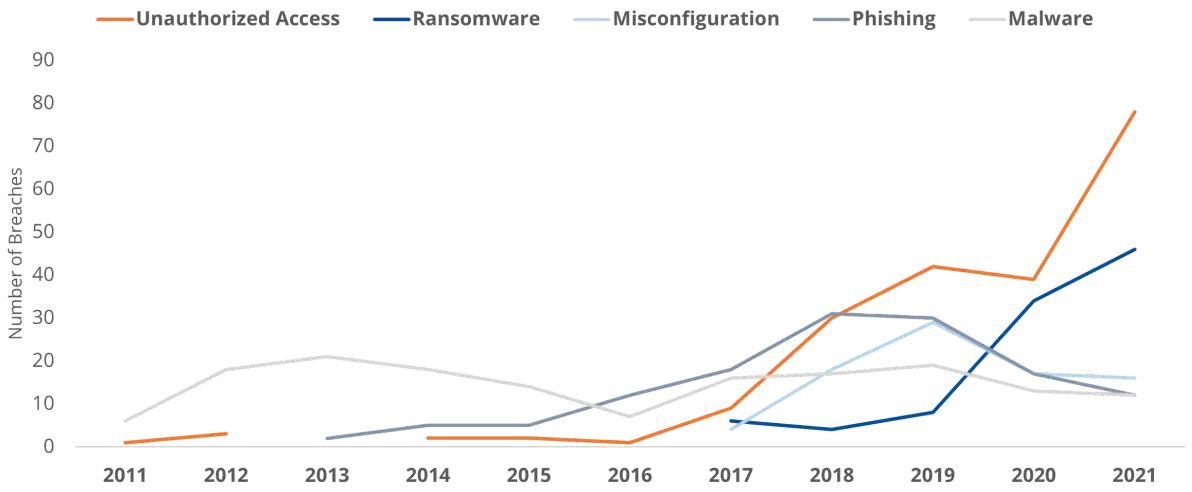
# TRENDS IN CYBERSECURITY INCIDENTS

## Types of Attacks




Since 2011, the most common type of cybersecurity breaches are related to unauthorized access, contributing to 21.2% of total disclosed attacks. The second most common type of breach since 2011 is malware incidents, contributing to 16.5% of total disclosed attacks. The third most common is phishing, contributing to 13.5% of breaches, followed by ransomware and misconfiguration.

In 2021, in line with the overall trend, the most common type of cybersecurity breaches related to unauthorized access, contributing to 41.5% of total disclosed attacks. Ransomware attacks in 2021 were the second most common type of cybersecurity incident, contributing to 24.5% of breaches disclosed during the year. This is significantly higher than the overall trend; ransomware is only the fourth most common attack type disclosed since 2011.




The number of disclosed cybersecurity breaches caused by unauthorized access has been increasing. In each of the last three years, the most common type of incident was unauthorized access breaches. This number skyrocketed in 2021, with unauthorized access contributing to 78 breaches disclosed during the year, compared to just 39 in 2020 and 42 in 2019.

The number of disclosed cybersecurity breaches caused by ransomware has also been increasing. In 2021, 46 breaches were attributed to ransomware attacks, compared to 34 in 2020 and 8 in 2019.

## Unauthorized Access Spotlight

Cybersecurity breaches classified as unauthorized access cover a wide range of attacks with various consequences. For example, in 2021, unauthorized access was attributed to the following breaches:

**Carver Bancorp [CARV]** disclosed a possible fraud incident involving the unauthorized use of a borrower's account through a third-party system.

The attack resulted in $2.1 million in fraudulent transactions. As a result of the attack, the company had to delay a quarterly filing in order to reassess its controls.

**Amtech Systems [ASYS]** disclosed a data incident that allowed attackers to gain access to and disable technology systems at one of its subsidiaries.

The attack had the potential to delay shipments to customers.

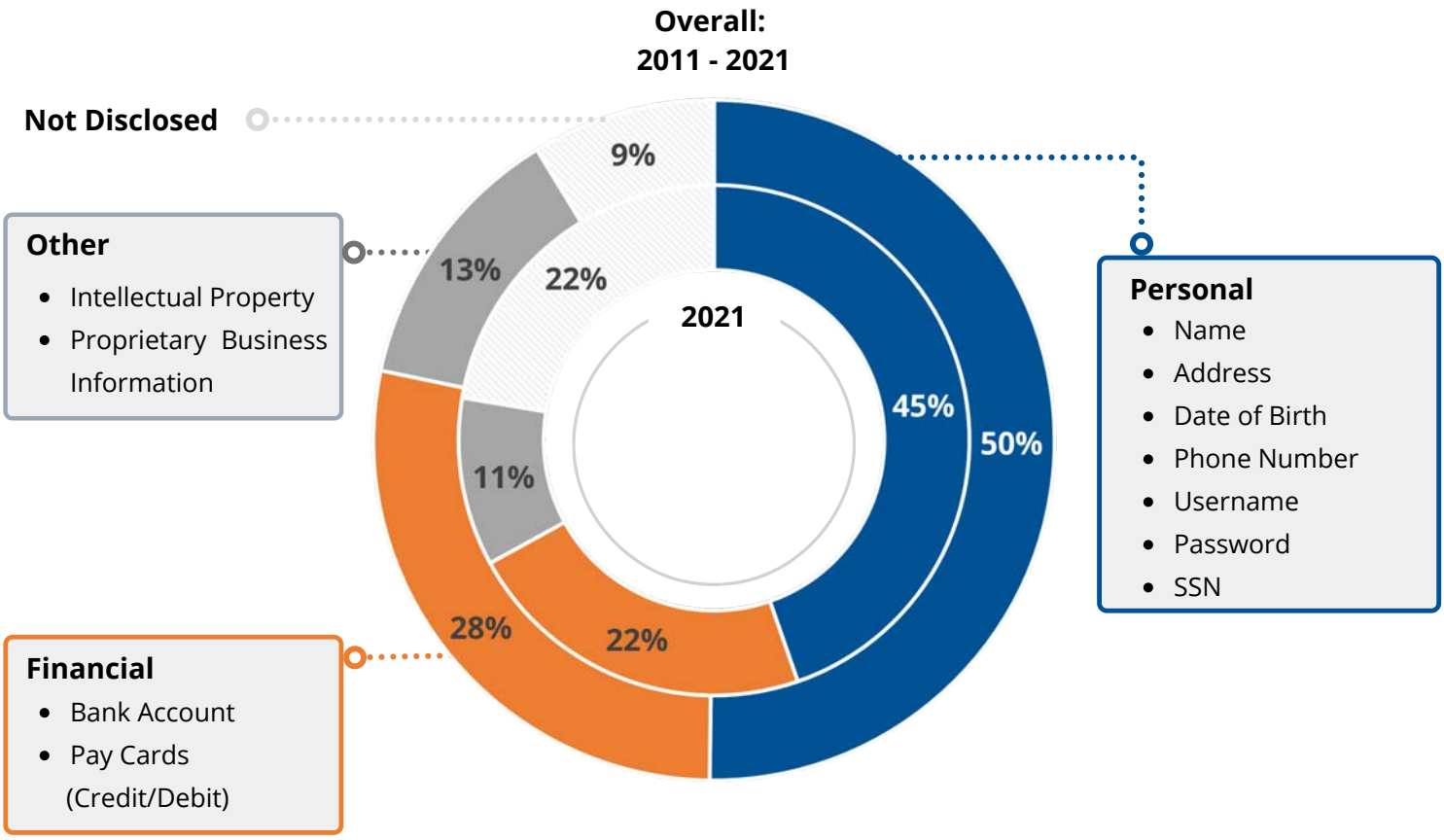
**Ubiquiti [UI]** disclosed that certain information technology systems were improperly accessed, compromising the company's source code.

The unauthorized party threatened to release the source code, potentially to the company's competitors, unless Ubiquiti made a payment.

## Types of Information

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

It's important to note not every type of attack will result in compromised protected information. For example, ransomware attacks often seek 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.




Since 2011, the most common type of information compromised in cybersecurity breaches was personal information, occurring in 50.4% of all disclosed attacks. The second most common type of information compromised since 2011 is financial, occurring in 28.0% of breaches.

Following the historical trend, the most common type of information compromised in 2021 cybersecurity breaches was personal information, occurring in 44.7% of attacks disclosed during the year. Financial information was compromised in 22.3% of breaches in 2021. 22.3% of breaches did not disclose the type of information compromised, aligning with an increase in ransomware attacks disclosed during the year.

Looking closer at the specific types of information compromised, the most common type in 2021 was personal names, disclosed as compromised information in over half (51.5%) of all breaches during the year. The second most common type of information compromised was social security numbers, occurring in 34.0% of the breaches.

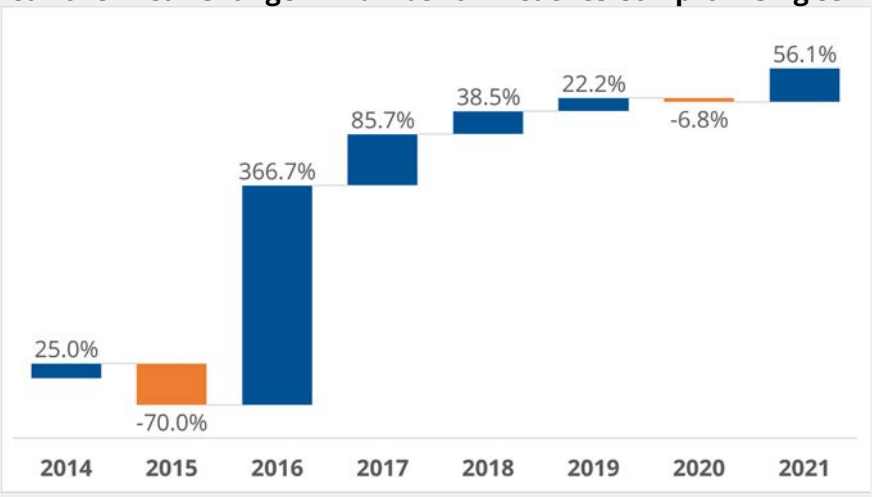
**Information Compromised in Cybersecurity Breach Disclosures**
represented as a percent of total breaches each year

| | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | 64.3% | 48.7% | 61.7% | 44.3% | 49.0% | 55.7% | 56.4% | 62.3% | 58.8% | 53.4% | 51.1% |
| SSN | 7.1% | 0.0% | 17.0% | 16.4% | 6.1% | 23.0% | 27.7% | 27.7% | 29.7% | 31.3% | 34.0% |
| Address | 25.0% | 7.7% | 12.8% | 18.0% | 32.7% | 31.1% | 37.2% | 38.5% | 30.4% | 29.0% | 28.2% |
| Email | 28.6% | 51.3% | 29.8% | 21.3% | 18.4% | 37.7% | 24.5% | 26.2% | 29.1% | 22.1% | 16.0% |
| Bank Account | 3.6% | 0.0% | 2.1% | 3.3% | 0.0% | 0.0% | 7.4% | 21.5% | 13.5% | 16.8% | 14.9% |
| Not Disclosed | 75.0% | 46.2% | 53.2% | 57.4% | 55.1% | 67.2% | 44.7% | 23.1% | 13.5% | 9.2% | 12.8% |
| Pay Card | 21.4% | 10.3% | 19.1% | 37.7% | 30.6% | 13.1% | 23.4% | 20.0% | 11.5% | 8.4% | 8.5% |
| Password | 25.0% | 59.0% | 31.9% | 23.0% | 20.4% | 31.1% | 7.4% | 11.5% | 8.8% | 12.2% | 4.3% |
| IP | 3.6% | 10.3% | 2.1% | 11.5% | 10.2% | 1.6% | 5.3% | 1.5% | 0.0% | 2.3% | 2.7% |
| User Name | 32.1% | 30.8% | 36.2% | 13.1% | 12.2% | 13.1% | 2.1% | 6.9% | 6.8% | 9.9% | 2.1% |

## Social Security Numbers Compromised in Cybersecurity Breaches

Breaches compromising social security numbers have continued to rise. In 2021, 34.0% of breaches compromised social security numbers, up from 31.3% of breaches in 2020. The percent of breaches impacting social security numbers has risen every year since 2016. Due to the sensitive nature of social security numbers, cybersecurity incidents that compromise this information are significant.

**Year-over-Year Change in Number of Breaches Compromising SSN**

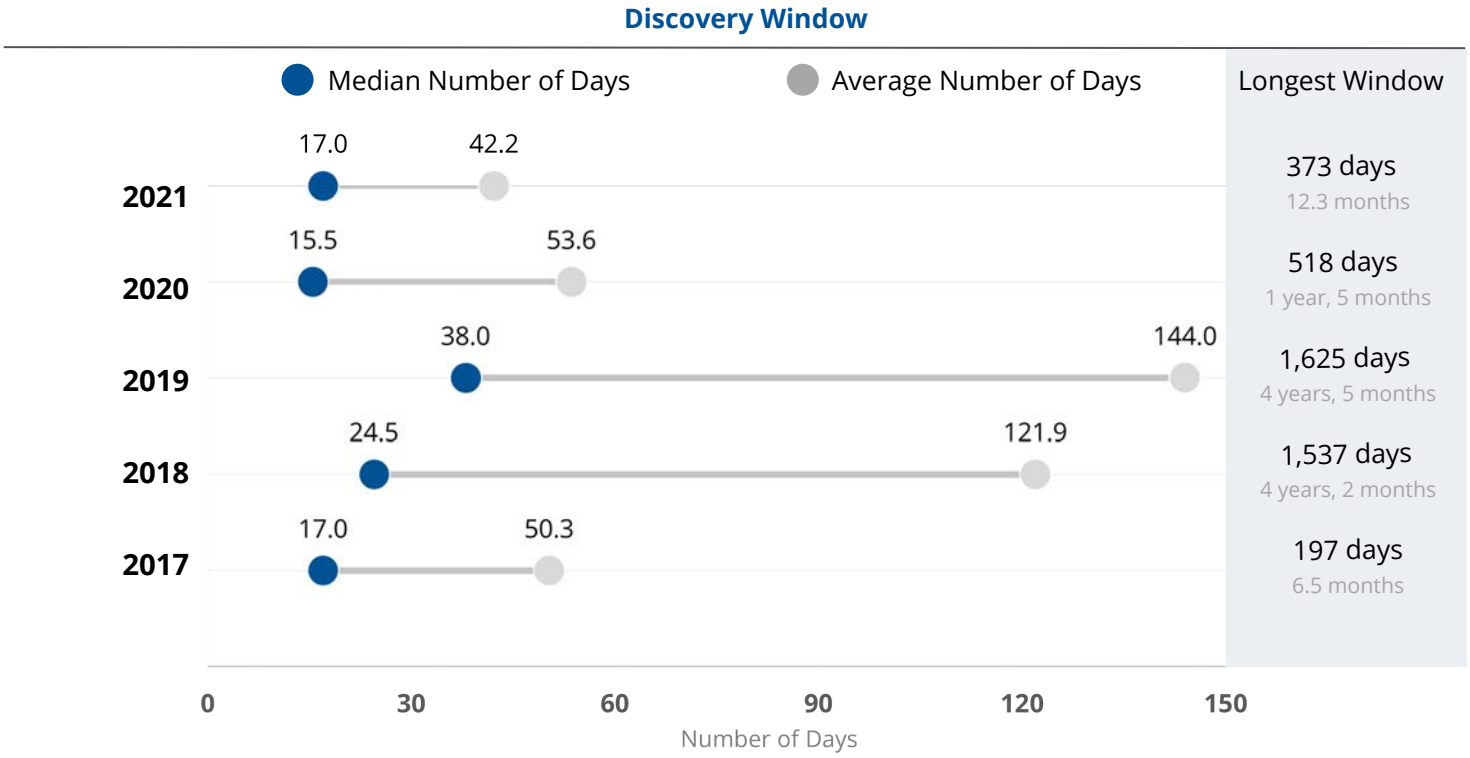


## Timeframe

*We look at the discovery and disclosure windows in two ways: the average and the median number of days in the window. The median is insulated from the high outliers in each year.*

### Discovery Window

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




Over the last five years, the average number of days it took for companies to discover a breach after it began was 92.6 days; the median number of days was 24 days.

In 2021, on average, it took 42.2 days to discover a breach, with a median of 17 days. The average in 2021 was less than 2020's 53.6-day average. The median discovery window increased slightly from 2020's 15.5-day median.

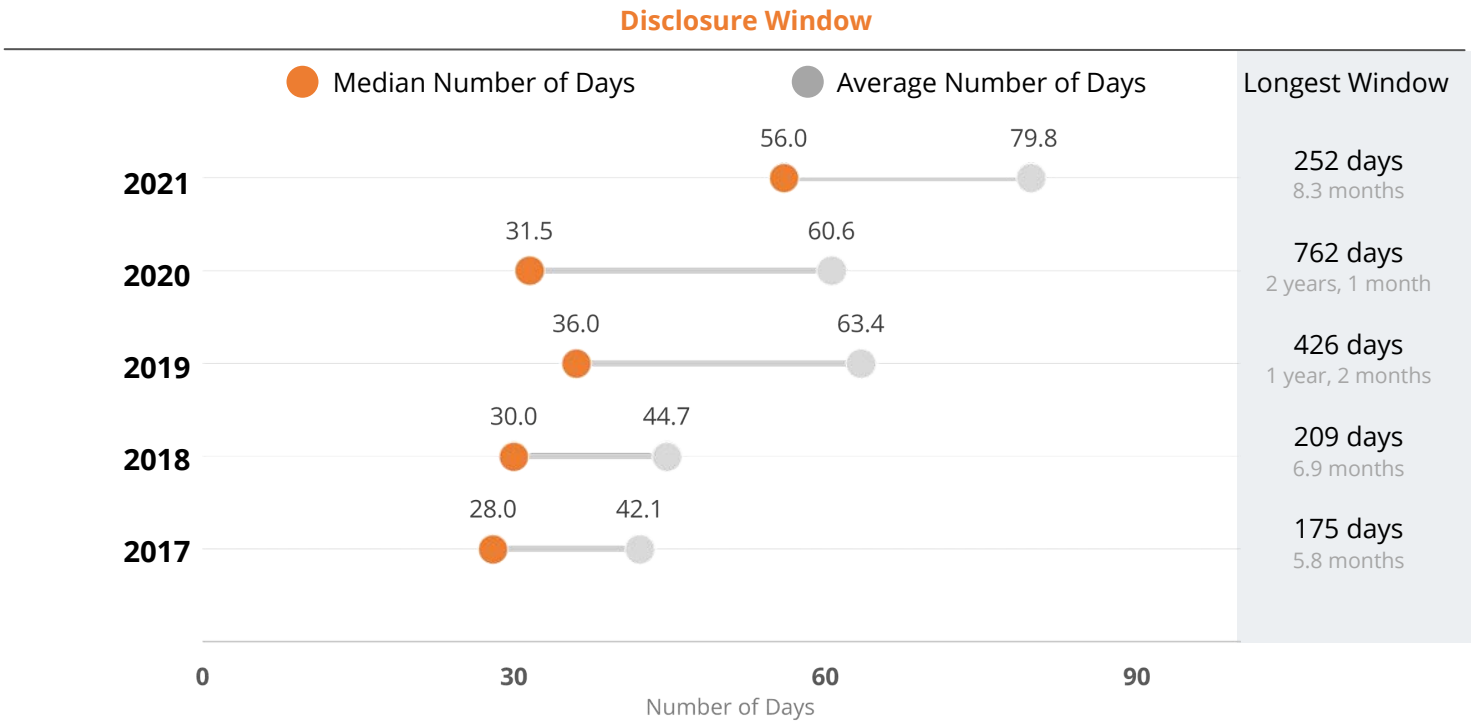
The longest discovery window in 2021 was 373 days, meaning it took over a year for the company (Golden Entertainment) to discover the breach. In comparison, the longest discovery window in 2020 was 518 days, just shy of a year and a half (Conduent Inc.).

## Disclosure Window

The SEC does not have disclosure requirements encompassing all cyber breaches. Instead, they provide guidance to "consider the materiality of cybersecurity risks and incidents when preparing the disclosure."[4] If a cybersecurity breach is expected to have material impacts, it must be disclosed within four days in a current report with the SEC (8-K filing).

Requirements for breach disclosures vary widely from state to state; many states require breaches to be disclosed "without unreasonable delay," but as there is no standard regulatory requirement, disclosure windows vary broadly. The disclosure window is considered the timeframe between when a breach was discovered and when it was first publicly disclosed.

A failure to timely disclose a cyber breach 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.[5] 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.




Over the last five years, the average number of days it took for companies to disclose a breach after it had been discovered was 58.5 days, with a median of 35 days.

In 2021, on average, it took 79.4 days to disclose a breach after being discovered, with a median of 56 days. 2021 had the longest average and median disclosure windows of the last five years.

The longest disclosure window in 2021 lasted 252 days, about eight months. In comparison, the longest disclosure window in 2020 was 762 days, or about two years and one month.

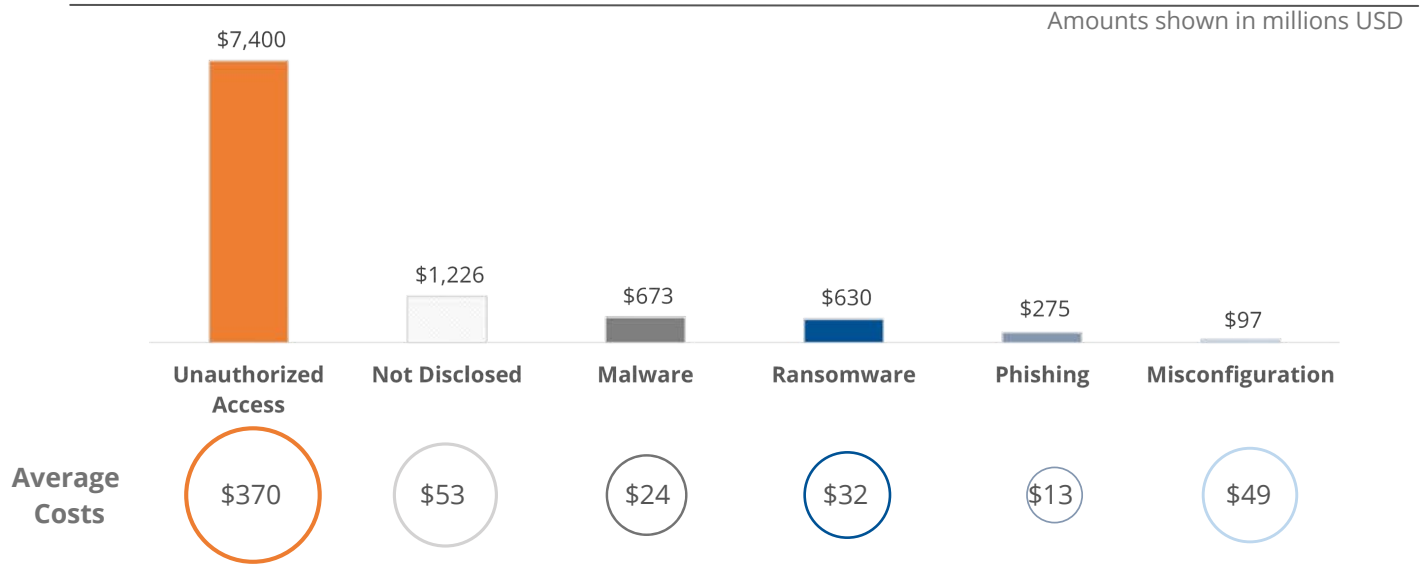
4 Securities and Exchange Commission. CF Disclosure Guidance: Topic No. 2 – Cybersecurity (October 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

5 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.

## Costs

Cybersecurity breaches can result in a litany of costs, such as investigations, legal fees, and remediation. There is also the risk of economic and reputational costs that can directly impact financial performance, such as reduced revenue due to lost sales.

### Total Costs by Type of Breach




Overall, unauthorized access cybersecurity attacks have the highest disclosed costs, totaling $7.4 billion since 2011. A distant second, totaling $1.2 billion in disclosed costs, are breaches of an unspecified nature. All other categories of cybersecurity breaches – malware, ransomware, phishing, and misconfiguration – have total disclosed costs of less than $1 billion, each.

Four out of the ten costliest breaches since 2011 resulted from unauthorized access. The unauthorized access breaches that impacted Meta Platforms (formerly known as Facebook) and Equifax in 2018 and 2017, respectively, cost the companies each over $1 billion.

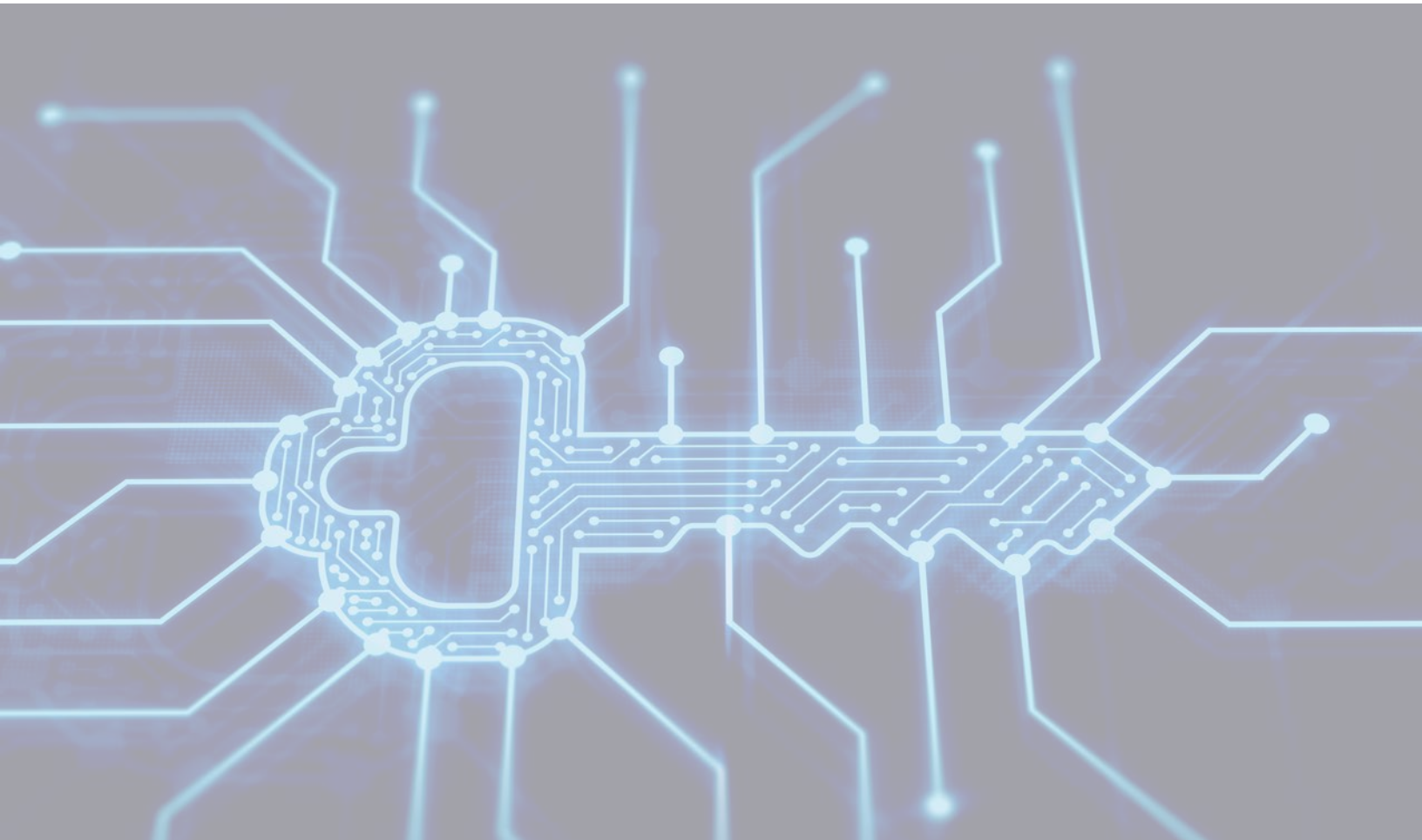
### Top 10 Costliest Breaches: 2011 - 2021

| Company | Year | Total Costs (in millions) | Type of Breach | Information Accessed |
|---|---|---|---|---|
| 1. Meta Platforms | 2018 | $5,100 | Unauthorized Access | ND |
| 2. Equifax | 2017 | $1,703 | Unauthorized Access | Address \| Pay Card \| Name \| Other \| SSN |
| 3. Natura & Co | 2020 | $454 | ND | ND |
| 4. Merck & Co | 2017 | $330 | Ransomware | ND |
| 5. Home Depot | 2014 | $298 | Unauthorized Access | Pay Card |
| 6. Target | 2013 | $292 | Malware | Pay Card \| Other |
| 7. Marriott International | 2018 | $176 | Unauthorized Access | Address \| Pay Card \| Name \| Email \| Other \| Phone # |
| 8. Sony Group | 2011 | $172 | ND | Address \| Pay Card \| Name \| Email \| Other \| Phone # |
| 9. Altaba | 2016 | $159 | ND | Name \| Email \| Other \| Password \| Phone # |
| 10. Anthem | 2015 | $131 | Phishing | Address \| Name \| SSN |

Only 16 breaches disclosed in 2021 specified costs. 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 financial harm.

**2021 Cybersecurity Breaches:**
**Costs Exceeding $1 million**

| Company | Total Costs (in millions) | Type of Breach | Information Accessed |
|---|---|---|---|
| 1. Coinbase Global | $25.1 | Misconfiguration | Other |
| 2. Sinclair Broadcasting Group | $24.0 | Ransomware | Other |
| 3. TTEC Holdings | $19.3 | Malware | Name \| SSN |
| 4. Ardagh Group | $15.0 | ND | ND |
| 5. Fortress Biotech | $9.5 | ND | Other |
| 6. Sierra Wireless | $9.0 | Ransomware | Other \| SSN |
| 7. Carver Bancorp | $2.1 | Unauthorized Access | Other |
| 8. Amtech Systems | $1.1 | Unauthorized Access | Address \| Name \| Other \| SSN |
| 9. First Horizon Corp | $1.0 | Unauthorized Access | Bank Account \| Other |



# DATABASE OVERVIEW AND METHODOLOGY

## OVERVIEW

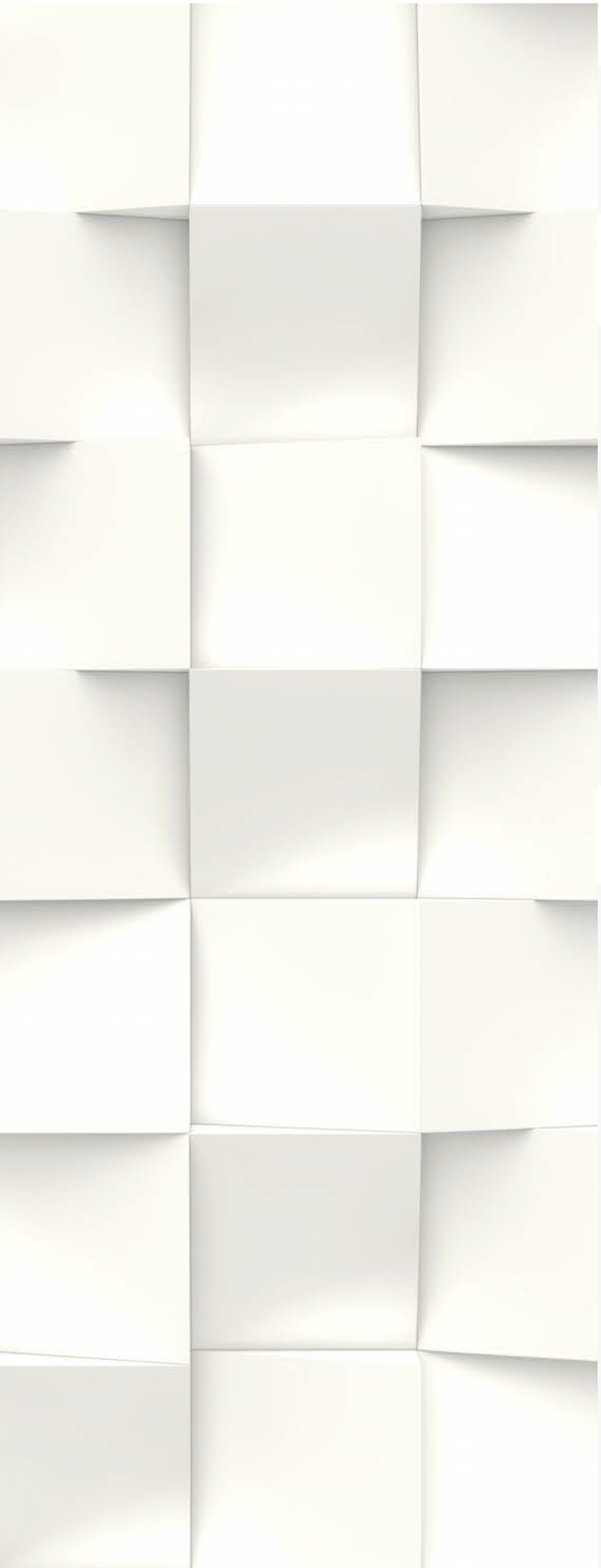
The Audit Analytics Cybersecurity database can be used to track the disclosure of and impacts arising from cybersecurity data breaches affecting public companies. This database makes it easy to locate the earliest public disclosure and provides updated details related to the breach on an ongoing basis, 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 2021.

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

Derryck Coleman - Director of Research Analytics
Madeleine Conley - Senior Research Analyst
Nicole Hallas - Senior Research Analyst

# ABOUT US

Whether for market intelligence, risk management, compliance, or research and public policy, 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 to find what they need to know. We are trusted to simplify the complex; to illuminate trends; and to reveal actionable insights.

# CONTACT US

Audit Analytics®
an Ideagen solution

**North America**
9 Main Street | Suite 2F
Sutton, MA 01590

Phone: 508.476.7007
Email: info@auditanalytics.com