AUDIT ANALYTICS®

TRENDS IN CYBERSECURITY BREACH DISCLOSURES

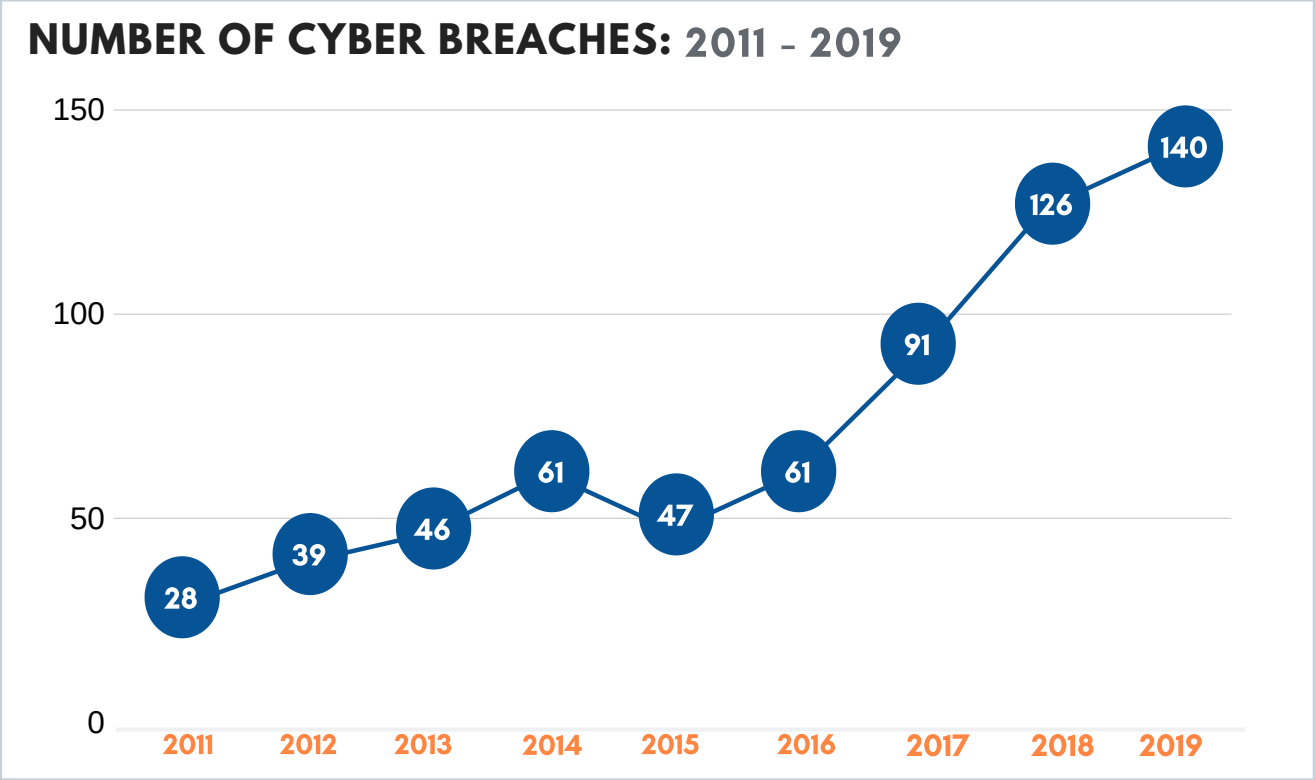
MAY 2020

An analysis of cybersecurity breaches affecting public companies from 2011 - 2019.

INTRODUCTION

It should come as no surprise that cybersecurity breaches are growing; it aligns with the greater use of computer technologies to conduct business.

Yet, how, when, and what businesses must disclose following a security breach varies depending on the entity requiring the disclosure. Each state has its own cybersecurity/data breach law, the Securities and Exchange Commission (SEC) has particular disclosure requirements for publicly traded companies, there are specific industry rules, and there are international laws that vary by country. Due to the lack of uniformity with disclosure requirements, there is a wide variety in the amount of information disclosed and the timeline of the disclosure.



140

overall cyber breaches
disclosed in 2019

11%

increase in breaches
since 2018

54%

increase in breaches
since 2017

LEVEL OF DETAILS DISCLOSED

The amount of details provided following a breach varies greatly: 43% of firms that reported a cyber breach since 2011 did not disclose the type of attack that was used to penetrate the company's systems.

Cyber attacks can be conducted using a variety of methods including:

- Exploitation
- Forged Cookies
- Malware or Ransomware
- Misconfiguration vulnerabilities
- Phishing
- Spoofing
- SQLi (SQL Injection Attack)
- Viruses

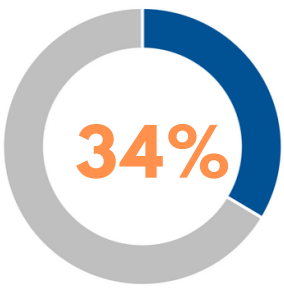
TYPE OF ATTACK

273	NOT DISCLOSED
125	MALWARE
90	PHISHING
75	UNAUTHORIZED ACCESS
45	MISCONFIGURATION
29	SQLi
4	EXPLOIT

MOST COMMON TYPES OF BREACHES

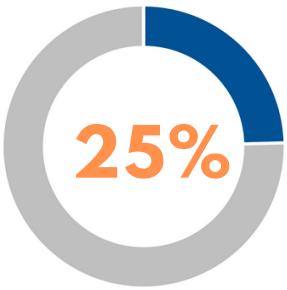
Of the companies that did disclose the type of attack, 91% were affected by **malware**, **phishing**, **unauthorized access**, **or misconfiguration vulnerabilities.**

Malware



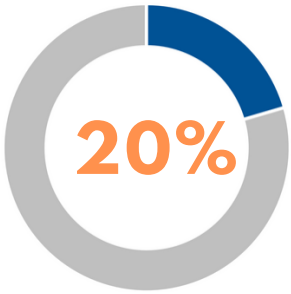
Malicious software intentionally designed to cause damage

Phishing



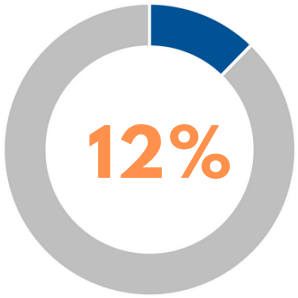
Fraudulent attempt to obtain sensitive information under guise of trustworthy electronic communication

Unauthorized Access



Unauthorized party gains access to protected systems and data

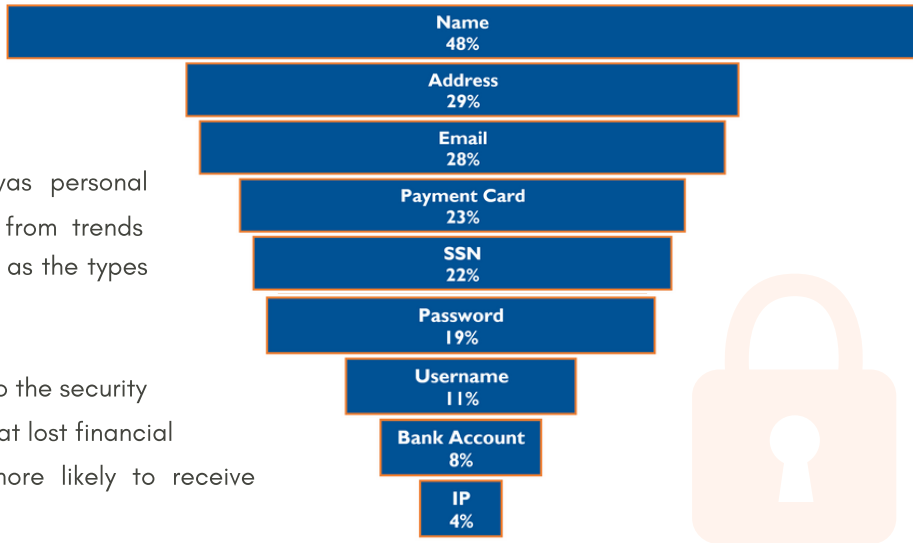
Misconfiguration



Exploitation of incorrectly assembled safeguards for web applications

INFORMATION COMPROMISED

There are nine pieces of information that hackers generally seek, ranging from personal to financial, as well as credentials such as usernames.



In 2019, the most frequently compromised data was personal information: names and addresses. This is a departure from trends seen through 2018, which saw names and credit cards as the types of information most often compromised.

The type of data stolen can influence market reaction to the security breach news. Investors are more likely to punish firms that lost financial information in a cyberattack, as these firms are more likely to receive significant fines and/or face legal action.

TOP NUMBER OF RECORDS COMPROMISED

		TYPE OF INFORMATION COMPROMISED					
		Credentials	Personal	Financial	Identifier	Number of	
Company	Date of Attack	Username, Password	Name, Address, Phone, Email	Bank Account, Payment Card	SSN	Records Stolen	= 250 million records
Yahoo Inc.	December 2016		●			3 billion	
First American Financial Corp.	May 2019			●	●	885 million	
Facebook Inc.	April 2019		●			540 million	
Yahoo Inc.	September 2016		●	●		500 million	
Huazhu Group	August 2018	●				500 million	
Time Inc.	May 2016	●	●			427 million	
Marriott International Inc.	November 2018		●	●		383 million	
Zynga Inc.	September 2019	●				218 million	

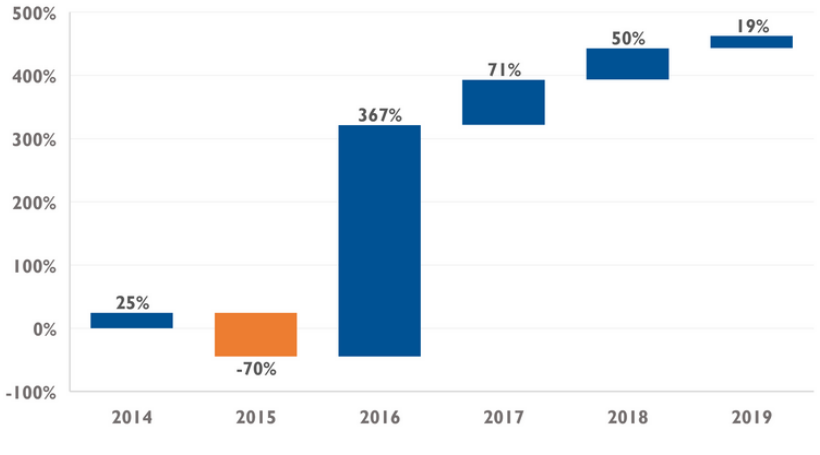
Social Security Number Breaches

Since 2014, the number of cyber attacks compromising Social Security numbers has drastically increased.

One possible explanation for this is that hackers are becoming more sophisticated and can target information that is most valuable, such as Social Security numbers.

CYBER BREACHES COMPROMISING SSN

% Change Year-over-Year



DISCLOSURE TIMEFRAME

The SEC does not provide specific guidance for disclosing a cyber breach, instead requiring companies to "consider the materiality of cybersecurity risks and incidents when preparing the disclosure."[1] Requirements for breach disclosures varies widely from state to state; many states require breaches to be disclosed "without unreasonable delay", but there is no standard regulatory requirement.

After reviewing publicly traded companies that have disclosed breaches since 2011, Audit Analytics found that it took an average of 108 days before companies discovered a breach and another 49 days, on average, before the breach was disclosed.

Number of Days to Discover Attack

108
AVERAGE

1,625
MAXIMUM

30
MEDIAN

Data breaches that are not discovered quickly raise red flags about a company's internal controls, suggesting that controls may not have been sufficient enough to detect the issues in a timely manner.

Once breaches are discovered, companies should be quick about disclosing the attack. Disclosure delays could trigger SEC action, such as the $35 million fine the agency levied against Altaba (f/k/a Yahoo) in April 2018. The SEC claimed Yahoo misled investors by failing to disclose one of the world's largest data breaches. In all, Yahoo eventually disclosed six separate breaches, which together, affected over 3 billion accounts. The Company learned about the breach caused by Russian hackers in August 2013, but did not disclose the breach to the public for years, until Yahoo was about to be acquired by Verizon Communications [NYSE: VZ] in 2016.

Number of Days to Disclose Attack

49
AVERAGE

456
MAXIMUM

30
MEDIAN

SEC Investigative Report

Cyber breaches that are not discovered quickly are concerning for both regulators and investors. On October 16, 2018, the SEC's Division of Enforcement issued an investigative report regarding cyber-related fraud's effect on public company internal controls.[2]

The report reviewed nine cases in which public companies' electronic communications were used to perpetuate fraudulent payments. The SEC did not recommend enforcement, but did recommend that companies reevaluate internal controls in relation to cyber threats.

Other companies have also waited more than a year to disclose information about a cyber breach once it was uncovered.

In 2019, Avid Technology Inc. [Nasdaq: AVID] notified customers that their information had been compromised over a year earlier, though some customers were notified within seven months of the incident. Avid's breach involved unauthorized access to employee email accounts, in which a rule to forward all incoming messages to an unauthorized email account was established.

Similarly, Forterra Pipe & Precast, a subsidiary of Forterra Inc. [Nasdaq: FRTA] notified consumers in April 2019 that a breach had occurred between January and October 2018, resulting from an email phishing campaign targeting employees. Forterra determined in January 2019 that an email attachment containing personal information may have been compromised, but consumers were not notified for another 3 months - 15 months after the attack began.

EXAMPLE: Lengthy Discovery

Company:
Choice Hotels International

Date of Breach:
June 2015 - November 12, 2019

Date of Disclosure:
December 2, 2019

Number of Times Breach Occurred:
88,000 times

Description:
Customer data that had been entered into an online reservation form on Choice's website was compromised due to a coding error affecting a certain web browser. If the web browser crashed as the customer was making a reservation, the information - including customer name, email address, state, zip code, country code, and the number and expiration date of the payment card - was inadvertently made accessible to third parties with whom Choice has a business relationship.

CASE STUDY: Capital One 2019 cyber breach

The 2019 cybersecurity incident for Capital One Financial [NYSE: COF] affected approximately 100 million U.S. consumers, and compromised information including 120,000 Social Security numbers, 80,000 bank account numbers, personal information required on credit card application forms such as names, contact information, dates of birth, and income, and customer status data such as credit scores and payment histories. In 2019, the exploitation attack cost Capital One $72 million to cover expenses including consumer notifications, credit monitoring, and professional support; the cost was offset by $34 million of insurance recoveries.

Type of Attack: Exploitation

Information Compromised:
Social Security Numbers
Bank Account Information
Personal Information

Days to Disclosure Attack: 119 days

Remediation Costs (to date): $72 million

Insurance Recoveries: $34 million

Contributing Factors to Longer Discovery Time After Cyber Breach

OVERALL AVERAGE: 108 DAYS

Industry

On average, companies in the **Transportation, Communications, Electric, Gas & Sanitary Services** industry took longer to discover a breach than other industries: **161 days**

Type of Attack

On average, **Exploit** attacks took longer to discover than other types of attacks: **584 days**

Type of Information Compromised

On average, when **Financial Information** was compromised it took longer to discover than other types of information: **156 days**

Contributing Factors to Longer Disclosure Time After Cyber Breach

OVERALL AVERAGE: 49 DAYS

Industry

On average, companies in the **Manufacturing** industry and **Finance, Insurance, and Real Estate** industry took longer to disclose a breach than other industries: **58 days**

Type of Attack

On average, **Phishing** attacks took longer to disclose than other types of attacks: **72 days**

Type of Information Compromised

On average, when **Personal Information** was compromised it took longer to disclose than other types of information: **60 days**

ACADEMIC CORNER:

Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets

by Amir, Levi, and Livine [3]

The amount of time it takes for companies to disclose attacks and how the public is made aware of these attacks may determine market reaction. A 2018 academic article using Audit Analytics data suggests that investors punish companies that delay breach disclosures or if the information is released by a third party, such as the media.

"We find that, in cases where firms immediately disclosed the cyber-attack, their equity value declined by 0.33%, on average, in the three days after disclosure and by 0.72% in the month after the disclosure. In comparison, the decline in market values was much larger in cases where firms did not disclose the attack and parties outside the firm later discovered it: 1.47% in the three days after the discovery of the attack, and 3.56% in the month afterward. ***These findings suggest firms withhold more severe cyber-attacks from investors.***"

COSTS

COSTS BY TYPE OF BREACH

Some attacks can result in economic costs, in addition to remediation costs. For example, Lumber Liquidators Holdings [NYSE: LL] experienced a network security incident in August 2019 caused by malware that encrypted certain information and impacted the ability of the Company to electronically process transactions. The Company remained operational during the incident and implemented manual processes to conduct sales, but Lumber Liquidators estimated the disruption to the sales process impacted total revenue in the range of $6 million - $8 million.

Additionally, Merck & Co. [NYSE: MRK] and Mondelez [Nasdaq: MDLZ] were impacted by malware in June 2017 that interrupted operations. Merck & Co. estimated lost revenues resulting from a 2017 breach amounted to $410 million through September 2018. Mondelez estimated roughly 0.4% of net revenue was lost on a full-year basis, or roughly $100 million.

On average, exploitation attacks have historically been the costliest breaches, with four attacks totaling $6.88 billion and averaging $2.29 billion. The 2016 cyber attack against Yahoo that used forged cookies to compromise 32 million user accounts cost the Company $79.0 million.

AVERAGE COSTS	$2.3 B	$79.0 M	$70.5 M	$38.5 M	$26.3 M	$21.3 M
NUMBER OF BREACHES	4	1	75	125	273	90
TYPE OF BREACH	Exploit	Forged Cookies	Unauthorized Access	Malware	Not Disclosed	Phishing
TOTAL COSTS	$6.9 B	$79.0 M	$493.7 M	$1.4 B	$627.6 M	$255.3 M

HIGHEST COSTS

In a previous analysis, Audit Analytics looked at the overall cost companies faced following a security breach.[4] The type of data stolen plays a noticeably large part; companies that lose financial data or Social Security numbers tend to face costlier remediation processes.

COSTS RELATED TO PAYMENT CARD AND BANK ACCOUNT BREACHES

$1.7 B	**EQUIFAX** September 2017 *Exploit*
$298 M	**HOME DEPOT** September 2014 *Unauthorized Access; Malware*
$292 M	**TARGET** December 2013 *Malware*
$176 M	**MARRIOTT** November 2018 *Unauthorized Access*
$114 M	**GLOBAL PAYMENTS** March 2012 *Not Disclosed*

Contributing to high costs of breaches involving payment cards and Social Security numbers are the services offered to consumers, such as credit monitoring, that may extend for years. Since this is sensitive information, it's also likely that companies will face consumer litigation.

Of public company breaches costing more than $50 million to remediate since 2011 , 7 breaches compromised financial information and 3 compromised Social Security numbers.

COSTS RELATED TO SOCIAL SECURITY NUMBER BREACHES

$1.7 B	**EQUIFAX** September 2017 *Exploit*
$131 M	**ANTHEM** February 2015 *Phishing*
$72 M	**CAPITAL ONE** July 2019 *Exploit*
$17 M	**CORELOGIC** December 2018 *Not Disclosed*
$7 M	**ROADRUNNER TRANSPORTATION** September 2018 *Phishing*

Contributing Factors to Costly Cyber Breaches

OVERALL AVERAGE COST: $116 million

Industry

On average, companies in the **Services** industry experienced the most costly attacks, though this is due in part to Equifax's costly 2017 breach: **$317 million**

Type of Attack

By far, **Exploit** attacks cost more on average. However, this includes the cyber breaches of Capital One's 2019 breach ($72 million), Equifax's 2017 breach ($1.7 billion) and Facebook's 2018 breach ($5.1 billion), some of the most costly breaches on record: **$2.3 billion**

This is followed by **Unauthorized Access** attacks, which includes the 2014 cybersecurity incident affecting Home Depot costing $298 million: **$151 million**

Type of Information Compromised

On average, attacks compromising **Personal Information** cost more: **$317 million**

This is followed by **Intrusions** - or forcible unauthorized activity on a digital network - which cost an average of **$115 million**

CASE STUDY: Equifax's 2017 cyber breach

In 2017, Equifax [NYSE: EFX] experienced a massive cybersecurity incident following a criminal attack that involved the theft of personally identifiable information of millions of consumers in the U.S., Canada, and the U.K.

Criminals exploited a software vulnerability in a U.S. website application and subsequently gained unauthorized access to Equifax's network between mid-May and July 2017. Once the activity was identified, Equifax acted to stop the intrusion and engaged a cybersecurity firm to conduct a forensic investigation.

Equifax's costs related to the 2017 cybersecurity attack - totaling $337.3 million in 2019 alone - were primarily related to costs to transform its information technology infrastructure and data security; legal fees and professional services costs to investigate the incident and respond to legal, government and regulatory claims; as well as costs to provide support to affected consumers. These costs have been partially offset by $125.0 million from cybersecurity insurance.

Type of Attack: Exploit

Information Compromised:
Social Security Numbers
Personal Information
Driver's License Numbers

Dates of Attack: May - July 2017

Date Disclosed: September 2017

Remediation Costs (to date): $1.7 billion

Insurance Recoveries: $125.0 million

On February 10, 2020, the U.S. Department of Justice announced that four members of the Chinese People's Liberation Army were indicted on criminal charges related to their involvement in the incident.

SECTORS IMPACTED

Of the eight different sectors reporting cyber attacks, the greatest number of breaches came from the **Services** and **Manufacturing** industries, with 184 and 155 breaches, respectively. One of the reasons for targeting these two sectors could be the large amount of financial information stored, such as credit card numbers.

53%

Cyber breaches reported by companies in Services or Manufacturing industries

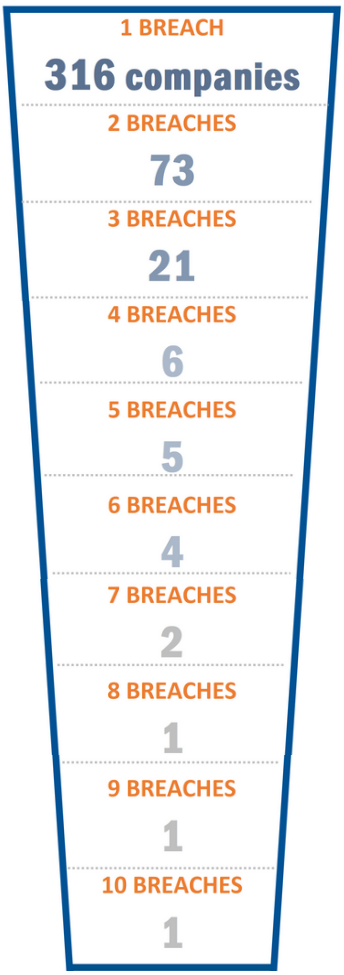
Services	Manufacturing	Finance, Insurance & Real Estate	Retail Trade	Transportation, Communications, Electric, Gas & Sanitary Services	Other
28.8%	24.3%	16.1%	14.2%	13.8%	2.8%

BREACHES PER COMPANY

It is important to keep in mind that companies may be re-victimized over time. Audit Analytics found that, while the majority of companies disclosed only one cybersecurity attack (316 companies), roughly 27% of companies were victimized on more than one occasion - indicating that cybersecurity threats are persistently present.

The 5 companies that have experienced 7 or more cyber attacks are all large companies with market caps over a billion dollars: Facebook [Nasdaq: FB], Sony [NYSE: SNE], Amazon.com [Nasdaq: AMZN], Comcast [Nasdaq: CMCSA], and T-Mobile USA.

Depending on what information is compromised or lost, multiple breaches can lead to additional costs in the future, such as litigation from consumers and vendors whose financial data was compromised, or internal employees whose information was affected.



26.5%

of companies that experienced a cyber attack
were victimized more than once

FOOTNOTES

[1] 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.

[2] Securities and Exchange Commission. Report of Investigation Pursuant to Section 21(a) of the Securities and Exchange Act of 1934 (October 16, 2018), available at https://www.sec.gov/litigation/investreport/34-84429.pdf.

[3] 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.

[4] Audit Analytics. Ranking the Equifax Data Breach (Updated) (November 1, 2017), available at https://www.auditanalytics.com/blog/ranking-the-equifax-databreach-updated/.

AUDIT ANALYTICS®

ABOUT AUDIT ANALYTICS

Audit Analytics is an independent research provider of audit, regulatory and disclosure intelligence. Through an easy-to-use online interface, Audit Analytics enables the accounting, legal, investment, and academic communities to analyze auditor market intelligence, public company disclosures, and risk indicators.

CYBERSECURITY DATA

Audit Analytics tracks cybersecurity breaches for all public companies since 2011 that are disclosed in news articles, public disclosures, regulatory filings and state websites.

9 Main Street, Sutton, MA 01590

508.476.7007

info@auditanalytics.com

www.AuditAnalytics.com