ExtraHop

THE TRUE COST OF A SECURITY BREACH

Cost Analysis of High Profile Data Breaches That Destroyed Earnings

SPECIAL REPORT

When a security incident occurs, it often results in a host of unexpected direct and indirect costs for the impacted organization. Those expenses may include the cost to hire a third-party digital forensics and incident response (DFIR) firm, the cost to remediate the incident, and the cost of new cybersecurity protections. But the true cost of a breach doesn't stop there. Victims of successful attacks can also suffer lost revenue, unplanned audit expenses, and can be hit with regulatory fines, legal fees, higher insurance premiums, reputational damage, professional crisis management and PR fees.

Despite the many and varied costs associated with a security incident, generally accepted industry research on the cost of a data breach focuses on the number of records stolen or people affected, which appears to have the effect of underestimating the true cost of a data breach. For example, IBM's Cost of a Data Breach Report from 2022 found the average cost of a data breach in the U.S. to be $9.44 million.[1] Meanwhile, security practitioners have seen about a dozen cases over the past four years in which the reported costs of various incidents have run into the hundreds of millions of dollars.

Then there's the impact on a company's earnings and stock performance. According to a 2021 study by Comparitech, companies reporting breaches tend to underperform the stock market.[2] The study also found that one year after the data breaches were reported, the companies' share price fell 8.6% on average and also underperformed the NASDAQ by 8.6%. The average share price of a breached company underperformed NASDAQ by 11.9% after two years and 15.6% after three.

On the pages that follow, we share in-depth research on the true, long-term costs of data breaches. To bring you these numbers, we combed through dozens of SEC filings in search of cost data that companies reported to investors and regulators. We triangulated the SEC data with news reports in the media. And we analyzed the impact of these breaches on companies' stock performance and quarterly earnings.

Net income for five of the organizations we studied sank an average of 73% within nine to 12 months of each organization announcing a breach. In addition, in nearly all cases, quarterly earnings declined and stock prices dropped significantly after data breaches. While economic and other business factors may have also contributed to sagging financial performance in some cases, there's no question these breaches impacted performance given the high costs companies reported.

We hope our research gives you a clearer and more accurate picture of the lingering, end-to-end financial impact of a data breach. It's our goal, in this time of economic uncertainty and belt-tightening, to arm you with data that you can use to make a bulletproof business case for investment in security controls to help your organization prevent and detect breaches before they lead to material business impact.

Net income... sank an average of 73% within nine to 12 months of each organization announcing a breach.

[1] Cost of a Data Breach 2022 [2] How data breaches affect stock market share prices

Data Breach No. 1

Size of Breach

More than **1 million** people

Impact on Earnings

The data breach had a significant impact on the company's financial results. In the first two quarters before the breach, the company reported quarterly net income of **$102 million** and **$166 million**. In seven of the next eight quarters, net income was down by either a double digit percentage from the same quarter a year earlier, or the company turned a net profit from a year earlier into a net loss.

Net income change timeline (by quarter)

(yoy)

Breach reported	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
↓27%	↑40%	↓41%	↓12%	↓60%	↓85%	↓712%	↓54%	↓64%

(quarters since breach announcement)

Impact on Stock Price

The company's stock price fell significantly after the breach was announced.

- The day after the breach was reported: stock price **dropped** about **21%**
- A week after the breach was reported: stock had **dropped** about **35%** from the price the day before the breach
- The stock stayed at a price **22% lower** than the price the day before the breach for two and a half months after the breach was reported

Reported Costs

Total cost, as reported by company
Over **$1 billion**

Multiple settlements with states
Over **$200 million**

Legal fees
Over **$80 million**
(Part of settlements)

Settlement reimbursing consumers
Over **$300 million**

Regulatory fines
Over **$100 million**

Settlement with businesses
Over **$5 million**

Cyber Insurance

The company's cybersecurity insurance reportedly paid for just **$125 million** of the costs, according to company SEC filings.

How the Breach Occurred

Attackers exploited a vulnerability in one of the company's databases to gain initial access. Attackers then moved from the database to other servers. On those other servers, attackers found usernames and passwords and used those credentials to access other systems. Attackers also encrypted data before exfiltrating it to evade detection.

Data Breach No. 2

Size of Breach

Tens of millions of records

How the Breach Occurred

Attackers gained access to the organization's network using stolen credentials. They then installed a backdoor, which enabled them to move undetected across the organization's network and harvest data from connected servers.

Reported Costs

Total cost, as reported by organization

Over **$900 million**

Identity theft protection

About **$400 million**

Identity and data breach monitoring contract

$500 million

Settlement to pay affected people

About **$60 million**

Internal costs

Unknown

*This breach did not take place at a publicly traded organization, therefore no income and stock price information is available.

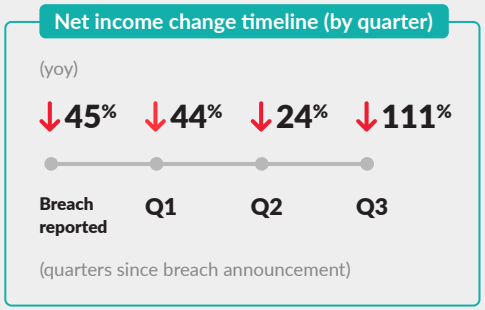
Data Breach No. 3

Size of Breach

More than **70 million** customers

Impact on Earnings

The company's net income dropped significantly in the quarters following the data breach.



Impact on Stock Price

The company's stock price dropped after the breach, although not immediately.

- Immediately after the breach, the stock price stayed near the same price for a week, then began a slow, steady decline.
- About a month after the breach announcement: stock price was **down 11%**
- Three months after the announcement: stock price was **down 19%** from the day before the breach announcement
- Five months after the announcement: stock price was **down** about **28%**

Reported Costs

Total cost

At least **$500 million**

Settlement of class-action lawsuit

About **$350 million**

Upgrades to cybersecurity practices

About **$150 million**

(an additional requirement in the lawsuit)

Internal costs

Not disclosed

Potential regulatory fines

Undetermined

Cyber Insurance

The company reported **$150 million** in insurance payments in filings to the SEC. It's possible that more insurance payments are still coming.

Data Breach No. 4

Size of Breach

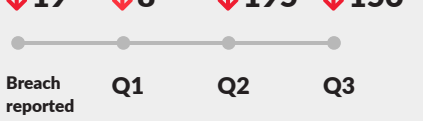
More than **100 million** customer records

Impact on Earnings

The company's financial performance took a hit immediately after the breach.

Net income change timeline (by quarter)

(yoy)



(quarters since breach announcement)

Impact on Stock Price

- One day after the breach announcement: stock price **dropped** by **7%**
- Two and a half weeks after the announcement: stock price was **down** about **15%**
- The stock price stayed more than **8% lower** for over a month, with the price not returning to the pre-breach price for four months.

Cyber Insurance

The company reported that it had cybersecurity insurance that covered some costs related to the breach, with a coverage limit of **$400 million** and a deductible of **$10 million**.

Reported Costs

Total cost

At least **$370 million**

Class-action lawsuit

$190 million

(about $55 million in attorney fees)

Fine from a U.S. regulatory agency

$80 million

Internal costs

$100 million - $150 million

(Including notifying consumers, providing credit monitoring services, and more)

How the Breach Occurred

The attacker used a home-grown software scanning tool to look for and exploit misconfigurations. The attacker obtained credentials from compromised servers, then, using the credentials, obtained access to data held on other servers. In addition, the attacker used a VPN and TOR to hide their location and identity, and make their activity appear as though it was coming from a legitimate, non-malicious computer.

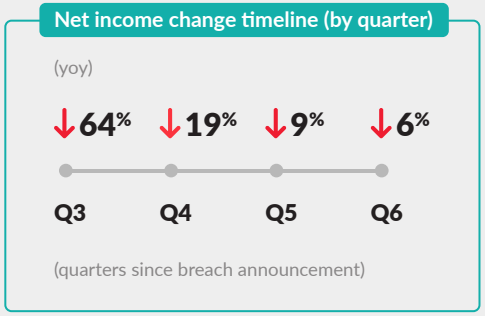
Data Breach No. 5

Size of Breach

Tens of millions of people

Impact on Earnings

The company reported small increases in net income from the previous year in the next two full quarters following the breach announcement.



Impact on Stock Price

Stock prices weren't negatively affected by the announcement of the breach or the announcement of the class-action settlement.

Cyber Insurance

The company didn't detail how much money it received from its insurance provider, although it did note in SEC filings that it had cyber insurance.

Reported Costs

Total cost

At least **$260 million**

Settlement of class-action lawsuits

$115 million

(Including $31 million in attorney fees)

Credit protection for consumers

About **$110 million**

Settlement with states

About **$40 million**

Initial notification costs

About **$30 million**

Regulatory fine

$16 million

How the Breach Occurred

Attackers sent spear phishing emails to employees. When an employee clicked on a hyperlink in the email, remote access malware was downloaded onto their computer.

Attackers then waited months before taking further action, eventually searching the company's network for personal and confidential business information. They allegedly stole data by placing it into encrypted files and sending it through multiple computers to destinations outside the U.S.

Data Breach No. 6

Size of Breach

Hundreds of millions of customer records

Impact on Earnings

The company's quarterly earnings took a significant hit after the breach was reported. While the COVID-19 pandemic likely had a major effect on income in the sixth, seventh, and eighth quarters following the breach announcement, it was not a factor before then.

Net income change timeline (by quarter)

(yoy)

Breach reported	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
↑36%	↓11%	↓65%	↓23%	↓12%	↓92%	↓201%	↓74%	↓159%

(quarters since breach announcement)

Impact on Stock Price

The company's stock price also fell after the data breach.

- On the day the breach was reported: stock price **down** about **6%**
- Three weeks after the breach was reported: stock price **down** about **17%** from the day before the breach was announced
- The stock price stayed at least **6% below** the price on the day before the breach for about two and a half months.

Reported Costs

Cost of the breach, reported by company

About **$160 million**

Regulatory fine

About **$25 million**

Cost of class-action lawsuits

Undetermined

(lawsuits were ongoing at the time this was published)

Cyber Insurance

Cyber insurance apparently paid for much of the cost of the breach. The company reported expected insurance payouts of **$132 million**.

How the Breach Occurred

Attackers used a remote access trojan (RAT) and a username and password sniffing tool to gain access to a privileged database.

THE NETWORK

Your Last Chance to Prevent a Data Breach

The data breaches described in this research highlight several common methods attackers use to gain access to organizations' systems while evading endpoint defenses. Some of these methods include exploitation of unpatched software vulnerabilities, exploitation of misconfigured hardware and software, and use of compromised credentials.

For attacks designed to circumvent endpoint defenses, tuning into the network can help security teams pick up on post-compromise activities like privilege escalation, network scanning and discovery, lateral movement, and command and control communication that signal an attack in progress. Detecting post-compromise activities via the network gives security teams an opportunity to stop attacks before they turn into costly data breaches.

The network provides a powerful source of truth and transparency into all users and assets across an enterprise–from cloud, to on-premises, to endpoints and remote locations. The network sees everything, shows everything, and leaves attackers with nowhere to hide.

A strong network detection and response (NDR) solution should leverage the power of the network and the packets it contains to automatically discover and classify all assets–whether managed or unmanaged–connecting to and communicating with it. A good network detection and response solution can also tell you what protocols and ports those assets use to communicate, and if any are suspicious or associated with known malicious IP addresses.

Without the ability to leverage machine learning to baseline normal network behavior and identify deviations from it; to perform continuous and on-demand packet capture to detect post-compromise activities; and to decrypt all east-west network traffic, organizations will continue to miss the telltale tactics and techniques that signal early-stage and mid-game attacks.

Using network intelligence to detect attacks in their earliest stages–when attackers are scanning for open ports and vulnerabilities, when they start using Active Directory to enumerate domain admin accounts, when they try elevating their privileges, or begin using Remote Desktop Protocol–is critical to preventing costly, damaging data breaches and avoiding unexpected security expenses.

Here are some specific tactics and techniques to look out for:

Using network intelligence to detect attacks in their earliest stages… is critical to preventing costly, damaging data breaches and avoiding unexpected security expenses.

Privilege Escalation

It is important to be able to detect privilege escalation in real time by building importance and privilege inference models for each device on the network and by monitoring for behavioral changes and changes in interactions with assets that require higher privileges.

Network Discovery

While attackers conduct many discovery activities directly on an endpoint using local command line tools or other local utilities, discovery activities (for example, account discovery, network service scanning, network share discovery, and file and directory discovery) are also often conducted remotely in ways that require communication across a network, making the network essential to revealing these signs of an early stage attack. To detect network discovery activities, it helps to analyze related network communications using an NDR solution with advanced machine learning. These NDR solutions identify the sometimes subtle behavioral changes that indicate an attack in progress. High-fidelity alerts, loaded with packet-level context, enable security teams to quickly and confidently respond.

Lateral Movement

Lateral movement is when attackers use the original host they've compromised to remotely access other devices on an organization's network, steal admin credentials, or otherwise increase their access to internal assets on the target network. To detect lateral movement, you need visibility into and the ability to decrypt and analyze internal, east-west traffic. Advanced NDR solutions offer out-of-band decryption that eliminates blindspots created by encryption, enabling security teams to track—and stop—attackers as they move laterally by detecting the following signs of lateral movement:

Remote Desktop Protocol (RDP): Attackers use RDP to manipulate systems whose credentials have already been compromised, or to expand access by using one compromised system to remotely control another inside the target network.

Windows Admin Shares: Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Attackers use this to expand access once they have compromised a valid account on a machine with access to administrative shares. Abnormal access to IPC$ indicates that this technique is being used.

Windows Remote Management: This is both a service and a protocol that allows users to remotely access a system.

Remote Services: An attacker who has access to a valid account will often use it to remotely access systems via Telnet or SSH and execute commands using stolen user credentials. The network provides visibility into this behavior.

Command and Control

Many common command and control (C2) TTPs require communication across the network, often using common ports. Watching the traffic on those ports, and understanding what constitutes abnormal traffic patterns, makes it much easier to detect C2 activity. For example, an attacker using a commonly open port for C2 may be transmitting using a protocol that is unusual for that port. By detecting which ports and protocols are in use and decrypting and analyzing the behavior patterns in this traffic, you can detect C2 activity despite the many tactics adversaries have developed to cover their tracks. Network intelligence, derived from analyzing network packets, can help you identify, investigate, and respond to the following signs of C2 activity:

Connection Proxy: Attackers may use proxies to piggyback on existing trust relationships or to obscure their tracks, making it more difficult for defenders to trace the true source of the attack. It is important to be able to analyze network traffic patterns to detect this and other types of C2 behavior.

Custom Command & Control Protocol: Attackers may develop their own protocols for command and control instead of using standard protocols. These custom protocols often mimic the behavior of standard application layer protocols, or specifically attempt to mask their behavior by taking advantage of traits of TCP/IP and the network stack. Ensuring real-time detection of unusual protocol behavior provides the necessary defense against these attacks.

Data Encoding: Adversaries may encode their C2 traffic using standard encoding schemes to evade detection. By analyzing traffic patterns, you can detect C2 regardless of the encoding scheme attackers use.

Data Obfuscation: To identify data obfuscation, look for malformed or anomalous data that passes across a connection, which indicates that the connection is being used for unapproved and potentially malicious purposes.

ExtraHop

Network intelligence, derived from analyzing network packets, can help you identify, investigate, and respond...

Can You Afford a $350 Million Data Breach?

The Business Case for Network Detection and Response

If you're relying on EDR, SIEM, and perimeter-based security tools to prevent data breaches, what are you going to do when an attacker evades those tools by using compromised credentials to gain access to your network? Similarly, what are you going to do when an attacker compromises an endpoint that doesn't have an agent installed on it, uses malware to remove or shut down endpoint agents, or disables SIEM logging? Would your SIEM alert your SOC analysts quickly enough to this kind of activity, or would your analysts have to sift through false positives and manually correlate security data from other tools to gain context and clear investigative insights?

These increasingly common attack scenarios call for 360-degree network visibility across on-premises, cloud and hybrid environments, asset discovery, continuous packet capture, and machine learning and decryption capabilities. Unlike logs and endpoint agents, the network can't be disabled, and there's no way for attackers to avoid the network.

A cybersecurity strategy that includes NDR alongside EDR, SIEM, and other security tools can give organizations much better chances of avoiding expensive and crippling data breaches.

Securing an organization can be a significant investment, but strong security tools are arguably much more cost effective than a massive data breach. Most companies can't afford a $1 billion data breach, let alone one that costs $350 million or even $9 million. As budget pressure continues, we hope the data we've provided on the cost and financial impact of different breaches helps you make a convincing case to your board of directors and executive leadership team for investment in cybersecurity to more effectively manage the risk associated with expensive data breaches.

Ready to see Reveal(x) in action?
Check out our self-guided demo

START DEMO →

ABOUT EXTRAHOP NETWORKS

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The ExtraHop Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they can see more, know more, and stop more cyberattacks. Learn more at www.extrahop.com