Office of Consumer Affairs and Business Regulation
MassCyberCenter at the MassTech Collaborative

Examining the Impact of *Data Breaches* in Massachusetts

mass.gov/consumer

masscybercenter.org

Examining the Impact of Data Breaches in Massachusetts

A Report by the Office of Consumer Affairs and Business Regulation and the MassCyberCenter

Introduction: The Growing Threat of Data Breaches

> "There are only two types of companies: those that have been hacked and those that will be." —*Robert Mueller, former director, Federal Bureau of Investigation (FBI)*

Over the last decade, data breaches have soared nationwide, putting billions of people at risk for scams, fraud and identity theft. In Massachusetts, companies are legally required to report data breaches affecting residents' personal information to the Office of Consumer Affairs and Business Regulation (OCABR) and to the Office of the Attorney General. OCABR publishes data breach reports and sample breach notification letters that were mailed to residents from companies to educate consumers about this growing threat and to help them verify if a letter they received is legitimate, rather than fraudulent. This data breach program is a vital resource for consumers and businesses as data analysis and trend discovery help everyone better guard against future incursions.

Any security incident in which unauthorized parties access confidential or sensitive personal data such as bank account information, Social Security numbers, passwords, healthcare details, corporate data including intellectual property, accounting records or customer information, is considered a data breach.

While numbers fluctuate annually, for 2024 alone, OCABR received 2,292 data breach submissions across industries that affected 4,448,136[1] Massachusetts residents. OCABR and the MassCyberCenter partnered to examine and analyze 2,164 of these breaches.[2] This deep data dive resulted in the following report that provides insight, implications and a pathway to better protection for businesses and individuals across the Commonwealth.

[1] This total does not equate to individuals as residents may have been victims of more than one breach.
[2] The MassCyberCenter analyzed breaches that occurred and were reported between January 1 – December 31, 2024. Breaches that occurred in 2024 but were submitted outside this date range were not included.

Key Findings Include:

- most incidents involved malicious or criminal conduct with system intrusion being the dominant threat vector
- financial services, healthcare, and banking represent the top industries affected
- organizations struggle with preventing, attributing and detecting breaches
- people, process, and technology contribute to data breaches through identified weaknesses such as insufficient multifactor authentication and passwords

Left to right: MassCyberCenter Director John Petrozzelli, SAIC's Cyber Center Senior Manager Jesse Jaramillo, formerly UMass Lowell Advisor Hans Olson, MassTech Collaborative Deputy Director Ben Linville-Engle, and CyberTrust Massachusetts CEO Peter Sherlock at MassCyberCenter's 2025 Cyber Forum.

Scope

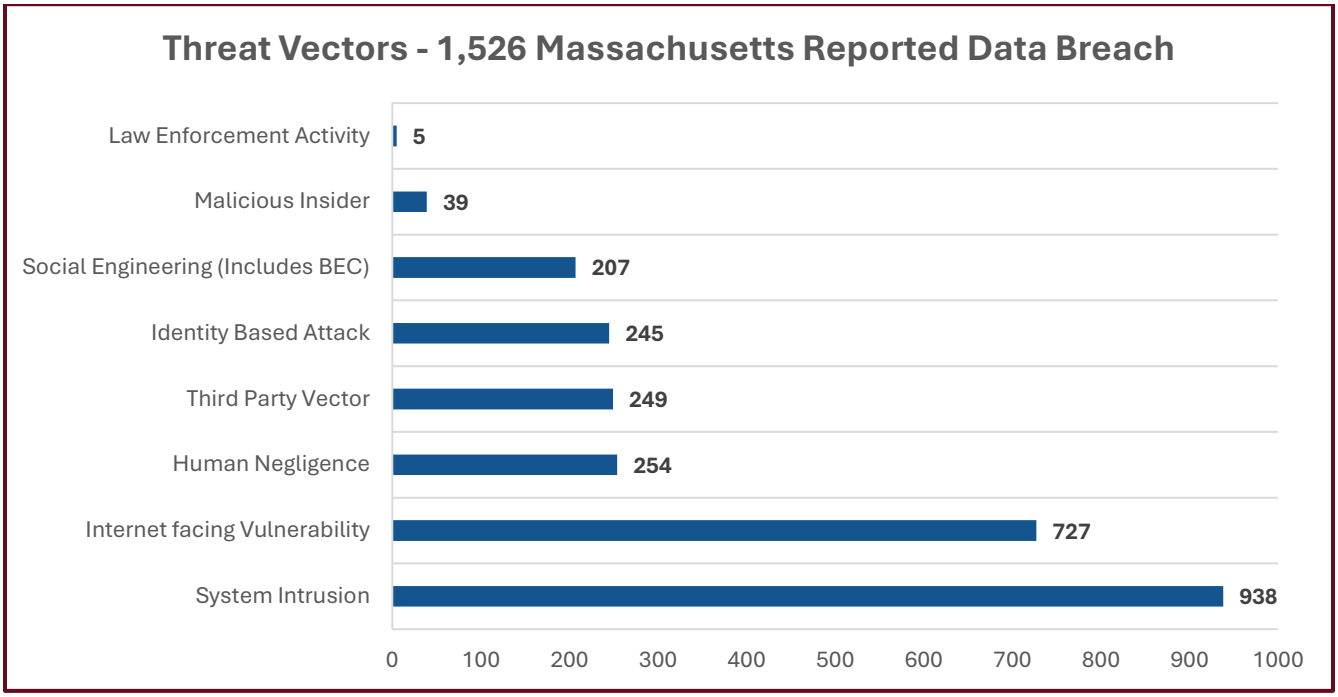
This analysis measures 2,164 data breaches that were reported to OCABR during 2024 and occurred between January 1, 2024, and December 31, 2024.

Methodology

Through a data sharing agreement with OCABR, the MassCyberCenter accessed limited information received by entities reporting data breaches that occurred in 2024 including business location and industry, type of breach, network configuration, incident narrative and response, number of residents affected, breach dates, as well as supplemental narrative letters. From this information, MassCyberCenter was able to extrapolate data, which it further analyzed to create this product. All work for this report was generated using Microsoft Excel worksheets and pivot tables. MassCyberCenter did not utilize artificial intelligence (AI) or any automated tools for analysis.

Out of the 2,164 incidents analyzed, approximately 1,526 contained enough information for MassCyberCenter to make a determination about the threat vectors attackers used to breach the data. During this process the MassCyberCenter viewed this data through the lens of "people," "process" and "technology" to identify weaknesses that may have led to these data breaches. The end of this report includes a summation of remediations certain companies enacted in response to these breaches. We hope this report will create a road map to protect Massachusetts businesses and residents in future years.

Threat Vectors



MassCyberCenter employees reviewed each incident to assess whether it occurred because of one of the following attack vectors:

Human Negligence

Definition: A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.[3] For the basis of this report, this category also included software design flaws.

Social Engineering, including Business Email Compromise (BEC)

Definition: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.[4] For an attack to be categorized as a BEC, also known as email account compromise (EAC), criminals must send an email message that appears to come from a known source making a legitimate request, like in these examples:

- A vendor sends an invoice with an updated mailing address.
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

Identity Based Attack

Definition: The set of physical and behavioral characteristics by which an individual is uniquely recognizable,[5] including identity theft, fraud and one or more of three types of incidents:

1. unauthorized use or attempted use of an existing account,
2. unauthorized use or attempted use of personal information to open a new account, or
3. misuse of personal information for a fraudulent purpose.

Definition: The intentional misrepresentation of information or identity to deceive others, the unlawful use of a credit or debit card or ATM, or the use of electronic means to transmit

[3] Massachusetts General Laws, Part I, Title XV, Chapter93H, Section1
[4] National Institute of Standards and Technology (NIST) definition for social engineering
[5] NIST definition for identity

deceptive information to obtain money or other things of value. Fraud may be committed by someone inside or outside the business and includes instances in which a computer was used to defraud the business of money, property, financial documents, insurance policies, deeds, use of rental cars, or various services by forgery, misrepresented identity, credit card or wire fraud.

Credit and Debit Card

If credit card account information was stolen because of a compromise, then that is considered an identity-based attack and a third party (see definition below). If a user reported a fraudulent transaction, that would only be considered identity fraud.

Malicious Insider

Definition: An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. [6]

System Intrusion

Definition: A security event or a combination of multiple security events that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.[7]

Internet-Facing Vulnerability

Definition: When unauthorized intruders gain access to networks, servers or computers through internet-facing software that has not been updated, virtual private networks with vulnerabilities, or software/hardware with vulnerabilities exploited by hackers before the vendor becomes aware of them (also known as a zero-day).[8]

Zero-day

Definition: Zero-day exploits are a security flaw in software or hardware that is unknown to the vendor and for which no patch or fix is available.

Third Party

Definition: This category refers to a breach where the vector was a third-party (not the organization reporting the breach) and was applied when credit card account information was stolen, or when a third-party company lost data belonging to the company that was a

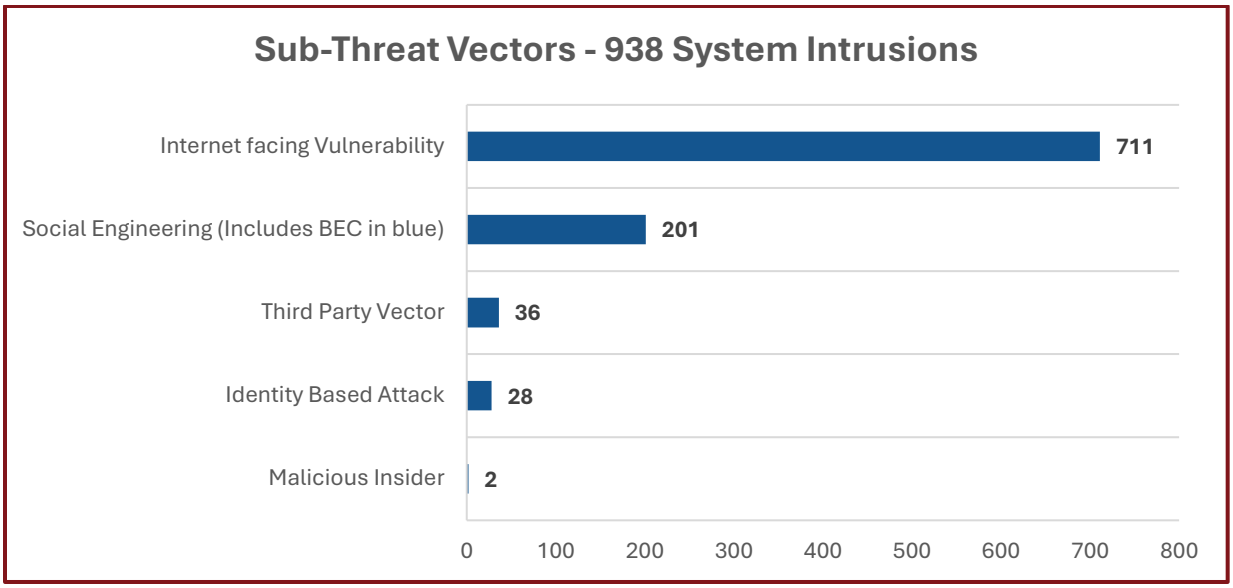
[6] NIST definition for insider
[7] NIST definition for intrusion
[8] NIST definition for vulnerability

victim of a breach. Third party in this case does not include the hackers, although many data breach reports use 'unidentified third party' to describe a hacker.

Law Enforcement Activity

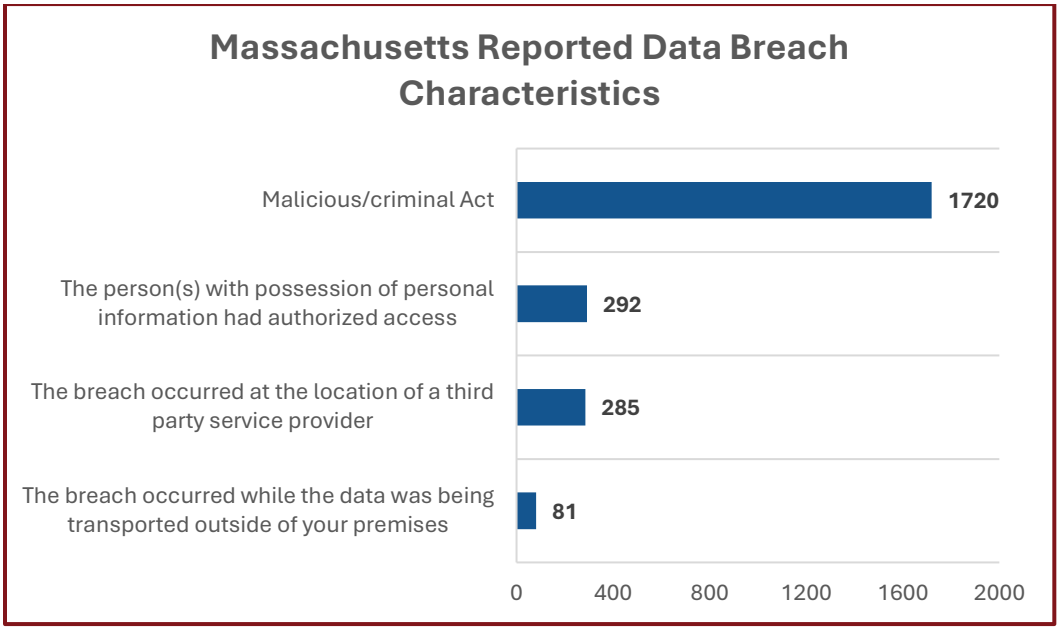
Definition: This category refers to when law enforcement, in the course of their duties, discovers victim's data on a piece of recovered evidence.

Sub-Threat Vectors Related to System Intrusions



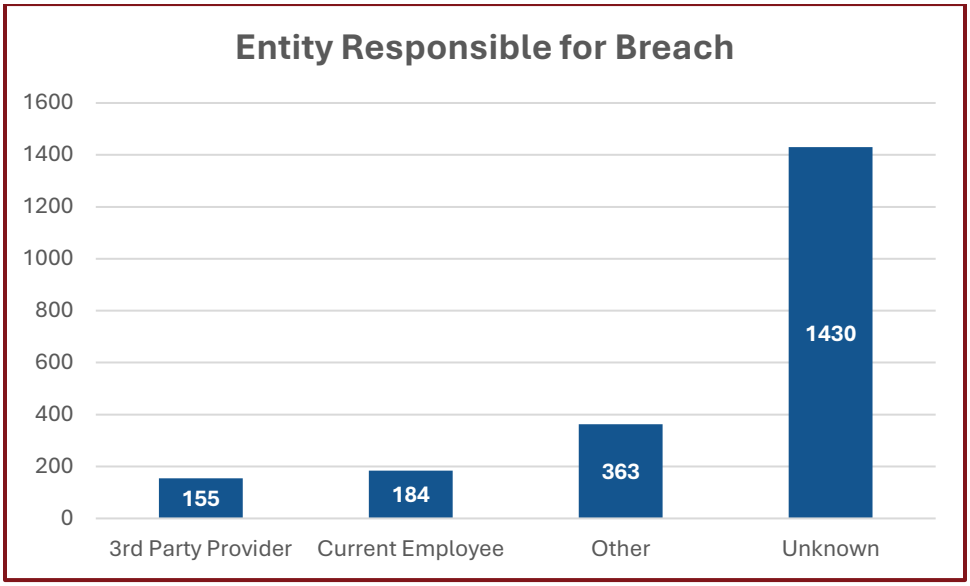
In the illustration above, MassCyberCenter reviewed sub vectors involving the 938 system intrusions. Many of these intrusions stemmed from internet-facing vulnerabilities (711) or social engineering attacks (201).

Massachusetts Reported Data Breach Characteristics



The overwhelming majority, approximately 1,720 of 2,164 incidents, included a malicious or criminal act. In 292 incidents, the individual with possession of personal information had authorized access. In 81 incidents the loss of data occurred while it was being transported outside of a company's premises. And in 285 incidents the breach occurred at the location of a third-party service provider (Note: That could have included compromise of an individual's credit card information).

Entities Responsible for Massachusetts Data Breaches

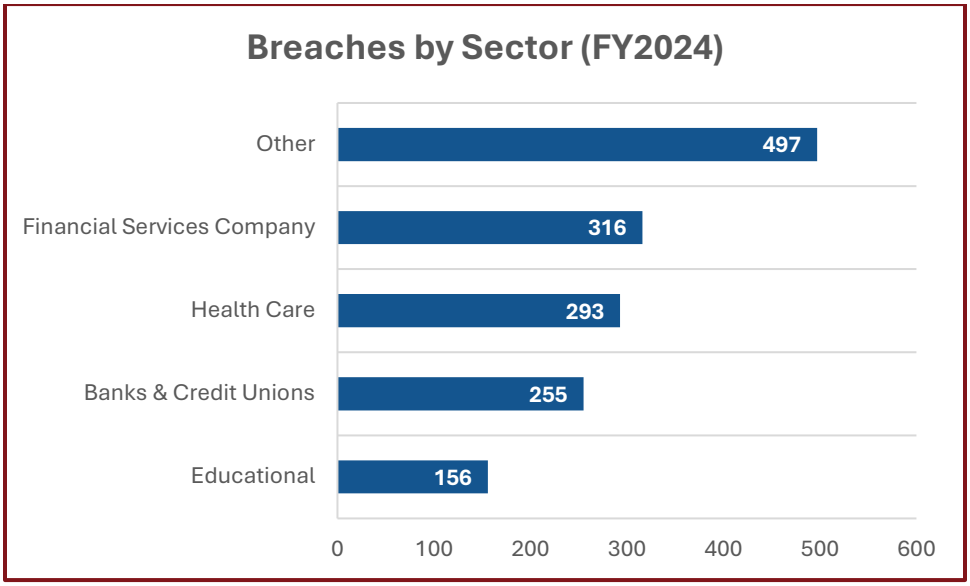


An analysis of breach attribution data reveals that the majority of incidents stem from sources that cannot be definitively classified, with “unknown or other” entities accounting for 1,793 cases.

This substantial category underscores persistent challenges in forensic visibility and attribution, particularly in complex or multilayered environments. In contrast, current employees were responsible for 184 breaches, highlighting the ongoing importance of insider risk management, access governance, and security awareness programs. Third party providers accounted for an additional 155 incidents, reinforcing the need for stronger vendor risk oversight and more rigorous controls across extended supply chains. Together, these findings illustrate that while internal and external actors both contribute to organizational risk, the largest exposure continues to arise from gaps in detection, monitoring and attribution capabilities.

An audience participant at MassCyberCenter’s 2025 Cyber Forum.

Breaches by Sector

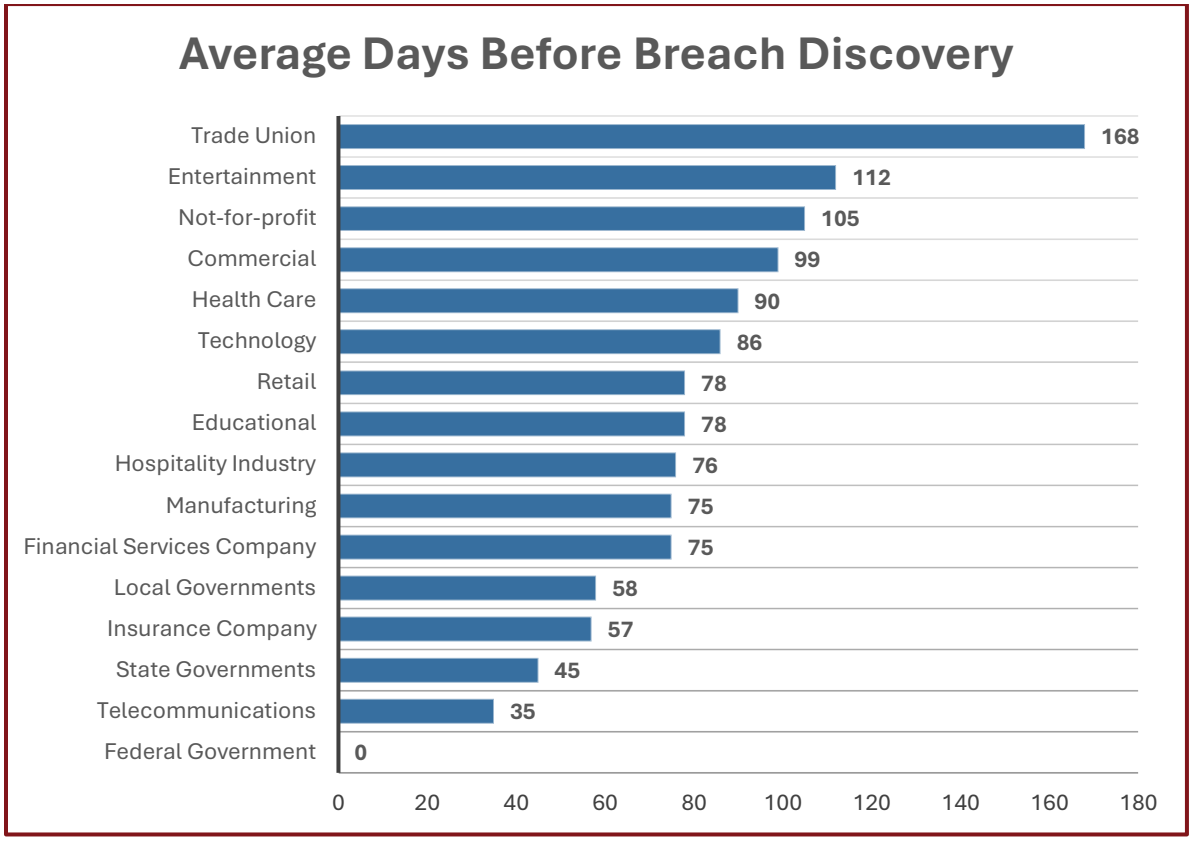


An analysis of breach incidents by sector shows that exposure is distributed across a wide range of industries, though some stand out as more frequent targets. The “other” category leads with 497 breaches, reflecting the breadth of organizations outside traditional regulated sectors that continue to face significant security challenges. “Other” may include regulated industries. However, the data is defined based on the submission from the reporting entity.

Among defined industries, financial services experienced 316 breaches, underscoring the persistent pressure on institutions that manage high-value assets and sensitive customer data. Healthcare organizations followed closely with 293 incidents, a reminder of how attractive medical data remains to threat actors and how operational complexity can widen attack surfaces. Banks accounted for an additional 255 breaches, reinforcing the need for sector-specific resilience strategies even within the broader financial ecosystem. Educational institutions reported 156 breaches, highlighting ongoing vulnerabilities tied to decentralized environments and diverse user populations.

Collectively, these patterns illustrate that while all sectors face meaningful cyber risk, the intensity and nature of that risk vary in ways that demand tailored security investments and governance approaches.

Days Until Discovery by Sector



The data shows significant variation in how quickly different sectors detect security breaches, highlighting uneven maturity in threat monitoring capabilities. These disparities may suggest that sectors with slower detection times may lack robust monitoring, incident response processes, or security visibility, increasing the likelihood of prolonged exposure and greater breach impact. It may also suggest how sophisticated the breach was and how difficult they are to detect.

Average Cost of Credit Monitoring Because of a Data Breach (< 5,000 residents affected)

A separate analysis shows that the average cost of providing affected citizens with credit monitoring services because of a data breach impacting under 5,000 residents is

approximately $1,185.[9] This highlights the disproportionate financial burden that even relatively small incidents can impose — especially on organizations with limited cybersecurity budgets. For companies that experience multiple attacks, the financial burden can increase significantly.

Average Citizens Affected

Threat Vector	Percent
Social Engineering	6%
Human Negligence	8%
Identity Based Attack	0.5%
Malicious Insider	0.2%
System Intrusion	71%
Internet Facing Vulnerability	65%
Third Party	4%

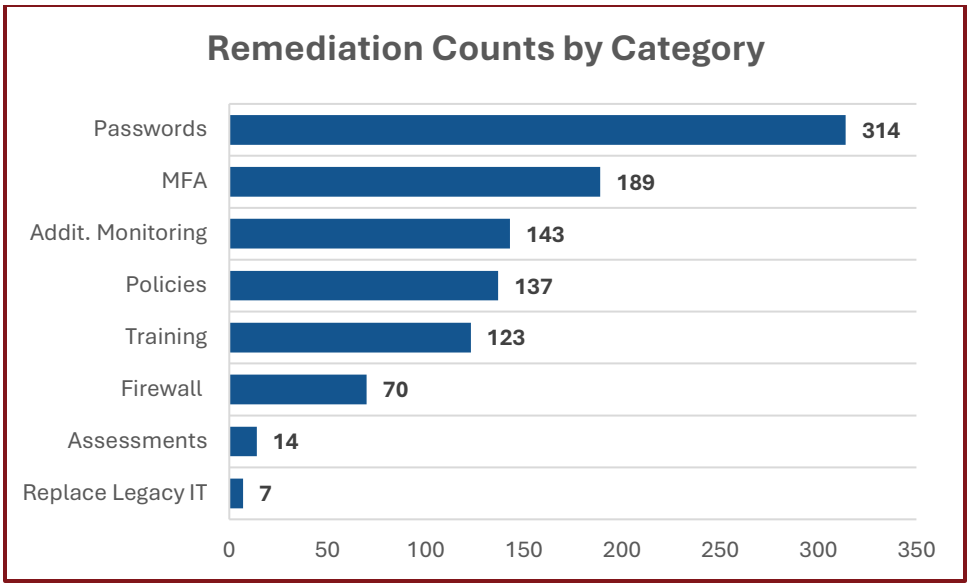
This chart provides analysis on the most prevalent threat vectors that caused breaches combined with the percentage of Massachusetts residents affected by those threat vectors.[10] System intrusions and internet-facing vulnerabilities were the two primary vectors that caused the majority of breaches and affected the most Massachusetts residents.

Remediation Steps

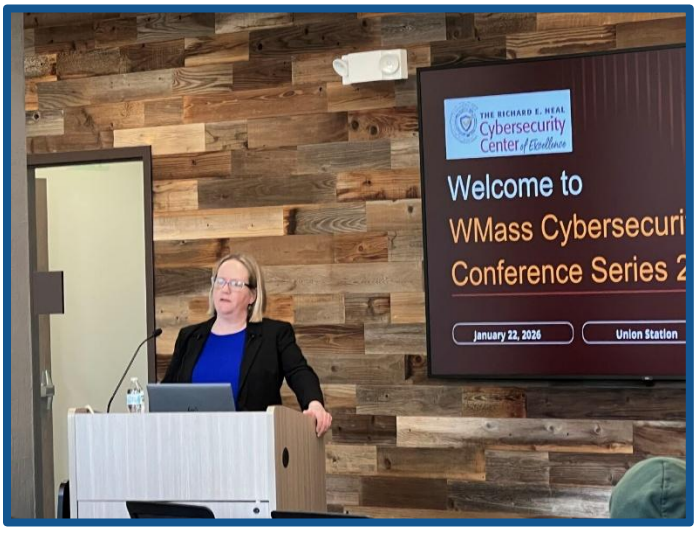
Across 2,164 incidents MassCyberCenter was able to determine 471 instances where companies identified remediations they were making to prevent future breaches. Remediations discussed in this section can help businesses and residents preemptively stop data breaches if implemented.

[9] MassCyberCenter conducted an independent analysis that included industry feedback to calculate the approximate average cost of $10 per affected citizen for providing credit monitoring services after a breach. Actual costs varied by organization.

[10] Percentages add up to over 100 because some breaches include multiple threat vectors.



In 32 percent of cases mentioned, people were strengthening passwords as a remediation to fix a vulnerability discovered during the breach. Multifactor authentication was the second most referenced remediation. Both remediations could be made for very little cost but could save companies millions of dollars in damages, while providing added protection to sensitive data. While reviewing these remediation categories, the MassCyberCenter identified weaknesses relating to people, process and technology that may have led to these data breaches.



OCABR Events and Outreach Manager Robin Putnam presenting at the Richard E. Neal Cybersecurity Center of Excellence on identity theft prevention and the importance of monitoring bank accounts, securing personal information, and reporting suspicious activity.

For businesses looking to strengthen data protection efforts, the MassCyberCenter developed a Minimum Baseline of Cybersecurity for Small Businesses, a strategy that aligns with the Center for Internet Security's (CIS) 18 Critical Security Controls.

Passwords (People/Process)

Passwords were the biggest change implemented by 32 percent of the companies represented in this report. Weak passwords are common and easily guessed by bad actors. For example, "minecraft," "qwerty," "123456," "admin," and "password"

were commonly used passwords in 2025, according to comparitech.com. Their top 20 list of the most common passwords for 2025 is as follows[11]:

Rank	Password	Number of Accounts
1	123456	7,618,192
2	12345678	3,676,487
3	123456789	2,866,100
4	admin	1,987,808
5	1234	1,771,335
6	Aa123456	1,411,847
7	12345	1,301,052
8	password	1,082,010
9	123	959,741
10	1234567890	674,200
11	12345678910	562,833
12	1234567	523,380
13	Aa@123456	501,446
14	Pass@123	485,846
15	Password	470,313
16	123123	385,949
17	P@ssw0rd	347,249
18	111111	326,154
19	admin123	306,343
20	1111	269,204

The most effective remediations for weak passwords would be for companies to adopt password managers, strong authentication policies, and modern multi-factor authentication such as passkeys. Employees should not use variations of the same password, and they should not mix their personal passwords with their work passwords.

Enforcing Multifactor Authentication (MFA) (People/Process/Technology)

[11] Comparitech, "The most-used passwords of 2025."

Of the companies represented in this report, 19 percent indicated that they would implement multifactor authentication (MFA) *after* the data breach occurred. In 2023, implementing MFA ensured almost 100 percent protection from fraud and criminal activity[12]. MFA should be implemented in internet-facing programs including virtual private networks, applications or productivity suites such as Microsoft Office 365 or Google Workspace. While MFA is effective, it must be part of a greater plan to protect a user or business.

Training (People/Process)

For businesses represented in this report, 12 percent indicated they would implement cybersecurity training *after* a data breach.

Often, specifically with social engineering that leads to data being compromised, humans can be identified as the weakest link. For example, a human clicks on a phishing email link or downloads a malicious file during an internet browsing session that allows unauthorized individuals access to personal or business data.

For cybersecurity initiatives to be implemented correctly employee training is critical. Annual cybersecurity training should be a priority for businesses. Employees should continually learn about the latest and greatest threats that could negatively impact their company and their personal lives.

OCABR and MassCyberCenter created a webinar as a training resource that provides an overview of cyber threats: Cybersecurity 101 - MassCyberCenter & Office of Consumer Affairs and Business Regulation.

Policies (Process)

Implementing policy changes *after* a data breach was referenced by 14 percent of the companies represented in this report.

Critical to cybersecurity compliance, policies dictate company actions and outline proper procedures for updating systems, onboarding and training employees, giving visitors access, confronting insider threats, and maintaining a positive and professional work environment.

Enhanced or Additional Monitoring (Process/Technology)

[12] Microsoft, "How effective is multifactor authentication at deterring cyberattacks?"

Implementing technical enhancements, in addition to protecting and upgrading internet facing vulnerabilities, was mentioned by 14 percent of companies represented in this study.

This includes upgraded endpoint detection and response, managed detection and response, and security information event monitoring solutions. These types of tools can assist in detecting or eliminating threats from ransomware groups, nation state actors, and financially motivated threat actors—if configured properly. Some of the best tools on the market have caught less than 10 percent of threats if not configured correctly. Massachusetts has a state-subsidized SOC/Range Initiative that provides Managed Detection and Response for a reduced price for local businesses.

Firewall Updates (Process/Technology)

In approximately 7 percent of remediations examined, breached companies found that firewall updates would be important to protect against future events. As we have shown in the data for internet-facing vulnerabilities, firewall and internet-facing software must be updated regularly and when zero-day exploits appear.

Replace legacy IT (Process/Technology)

In approximately one percent of breaches analyzed, legacy IT represented one of the issues that led to the data breach.

MassCyberCenter describes legacy IT as outdated computers or software running in an environment that is no longer updated by the original vendor. Another term for this is “end of life” software or hardware. The risk of using legacy IT in a company's environment increases over time because the vendors are no longer updating software, and any vulnerabilities will not be patched. Therefore, legacy hardware and software can be a very good entry point for hackers.

Assessments (People/Process/Technology)

In about one percent of breaches analyzed, conducting an assessment was referenced as a remediation. Assessments were cited to determine what vulnerabilities currently exist and where to focus limited resources with respect to strengthening technology and policy solutions. Assessment is an important first step for businesses looking to upgrade cybersecurity or IT systems.

Attorney General Andrea Campbell and OCABR Undersecretary Layla R. D'Emilia at UMass Amherst, discussing how Massachusetts consumers are affected by scams and fraud.

Conclusion

People. Process. Technology. One or all might open a door allowing unauthorized parties to access confidential or sensitive personal data. MassCyberCenter's analysis of 2,164 data breaches reported to OCABR during 2024 applied this lens to identify weaknesses that may have led to an unwanted intrusion. This dynamic demonstrates that cybersecurity is no longer confined to the technology department at any company, and now has core business, consumer protection, and public trust implications.

The analysis shows that while system intrusions, internet-facing vulnerabilities, and social engineering are major recurring threats to organizations, preventable less sophisticated weaknesses exist like access controls, employee awareness, and system maintenance.

Based on this sample, organizations show vast variation in the ability to detect, attribute, and respond to data breaches, putting sensitive data at greater risk for scams and fraud including identity theft. For businesses, even small incidents can lead to big costs when providing affected citizens with credit monitoring services.

Recommendations based on practical remediations cited by entities that reported breaches include:

- prioritizing a cybersecurity workplace policy;
- using stronger passwords and changing them frequently;
- implementing multifactor authentication and password managers;
- requiring employee training;
- implementing threat monitoring tools
- updating system security and firewalls; and
- replacing legacy IT (e.g., old computers and software).

While people, process, and technology may represent data breach gateways, they are also the key to implementing solutions that will help prevent future attacks.

About the Office of Consumer Affairs and Business Regulation

The Office of Consumer Affairs and Business Regulation (OCABR) protects and empowers consumers through advocacy and education and ensures a fair playing field for the Massachusetts businesses its agencies regulate.

OCABR oversees the state's Lemon Law Arbitration Program; Data Breach reporting; Home Improvement Contractor Registration, Complaints, Arbitration, and Guaranty Fund Programs; Do Not Call Registry; and Consumer Hotline as well as the Divisions of Banks, Insurance, Occupational Licensure, and Standards and the Department of Telecommunications and Cable.

Regarding consumer protection, OCABR's motto is, "knowledge is your best defense against fraud and scams," so the agency's goal is to educate consumers on how to protect themselves from crimes like data breaches, identity theft, and contractor scams – and what to do if they become a victim. Through virtual and on-site presentations, a consumer e-newsletter, social media campaigns, videos, and resources available at mass.gov/consumer, OCABR helps Massachusetts residents turn knowledge into power.

About the MassCyberCenter

The MassCyberCenter promotes the Massachusetts cybersecurity ecosystem by working to build a strong cyber talent pipeline and to strengthen the defense of local communities. The MassCyberCenter works with cities, towns, universities and the private sector to build

cyber awareness, institute best practices, grow future workforce talent, and create a more powerful cyber defense force to guard against future threats. Learn more at masscybercenter.org.