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

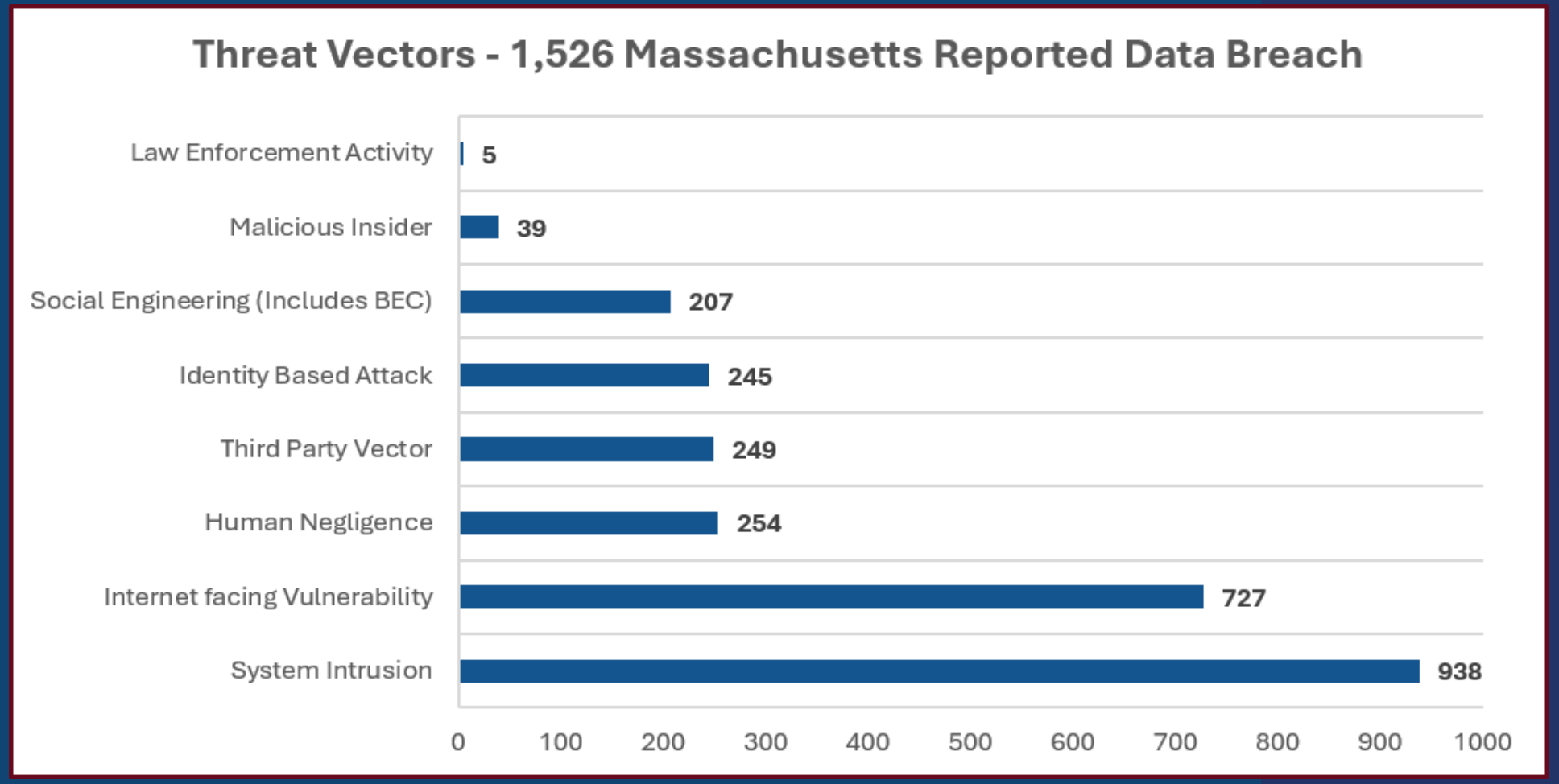
Examining the Impact of *Data Breaches* in Massachusetts

mass.gov/consumer masscybercenter.org

First-ever Data Breach Report

- In 2024, OCABR received **2,292** data breach submissions that affected **4,448,1361** Massachusetts residents.
- **2,164** of these breaches were examined.
- Top industries affected:
  - Financial services (316 breaches)
  - Healthcare (293 breaches)
  - Banking (225 breaches)
- #1 Threat vector: System intrusion

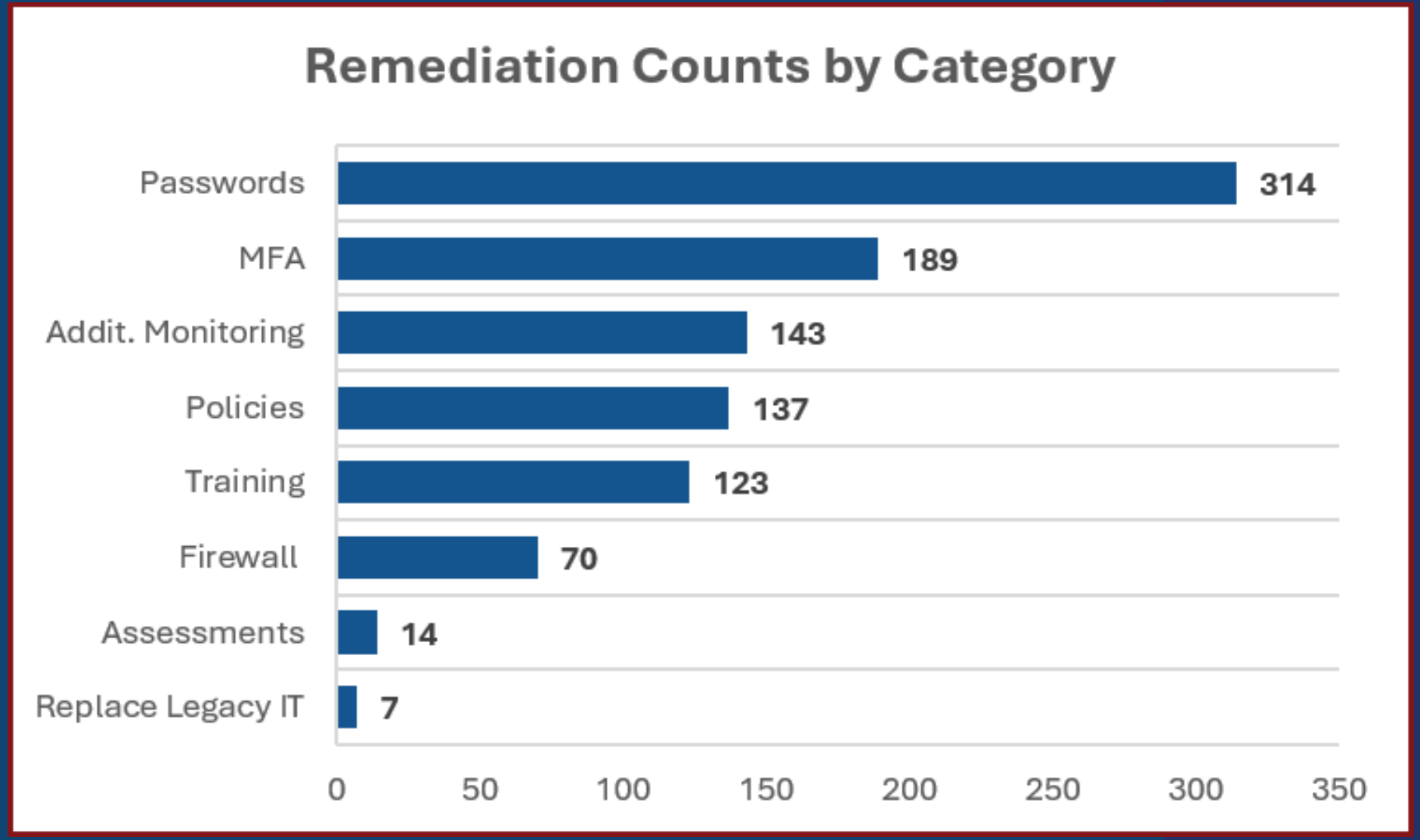
Average Time to Discover a Breach: 77 Days



Top threats:

- System intrusion
- Internet facing vulnerability
- Human negligence

Remediations: Low-cost fixes, high impact



- Passwords
- MFA
- Policy

Time it takes a hacker to crack your password 2024

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	1 hour	3 hours	6 hours
6	Instantly	1 hour	3 days	1 week	2 weeks
7	Instantly	1 day	5 months	1 year	3 years
8	21 mins	4 weeks	21 years	85 years	225 years
9	3 hours	2 years	1k years	5k years	15k years
10	1 day	55 years	56k years	327k years	1m years
11	2 weeks	1k years	2m years	20m years	77m years
12	5 months	37k years	152m years	1bn years	5bn years
13	4 years	968k years	7bn years	78bn years	378bn years
14	39 years	25m years	412bn years	4tn years	26tn years
15	390 years	654m years	21tn years	300tn years	1qd years
16	3k years	17bn years	1qd years	18qd years	129qd years
17	39k years	442bn years	58qd years	1qn years	9qn years
18	390k years	11tn years	3qn years	71qn years	635qn years

Hive Systems

Read more and download at hivesystems.com/password

Use Memorable 15-20 Character Passwords

- Never reuse passwords across accounts
- Store unique credentials in a password manager
- Use biometrics for secure, convenient vault access
- Consider passkeys instead of passwords
- Check exposed emails on HaveIBeenPwned.com

Multifactor Authentication

- Multifactor Authentication (MFA) is an authentication method that requires users to provide two or more verification factors to gain access to a resource.
- Use a reputable authenticator app instead of an email or text-based authentication.
- If you already use MFA, review any request carefully to avoid a hacker stealing your login sessions.
- Business owners should consider implementing number matching and adding login context to “push” notifications from authenticator apps.

Monitoring & Training

Technical monitoring tools strengthen defenses — but configuration is critical:

- 14 percent of companies reported implementing technical security enhancements.
- Defense in Depth will help when your tools are part of a unified defense.

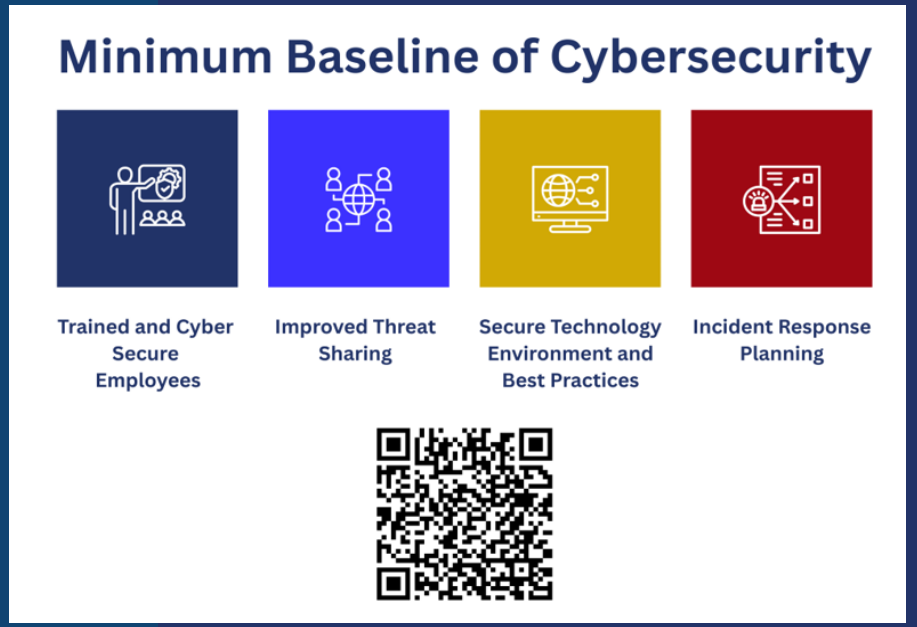
Continuous training turns employees into a stronger line of defense:

- 12 percent of businesses planned cybersecurity training after a data breach.
- Effective cybersecurity depends on employees recognizing and reporting threats.

Policies

Clear policies turn cybersecurity expectations into consistent action:

- 14 percent of companies reported implementing policy changes after a data breach.
- Strong policies establish accountability and support cybersecurity compliance.
- Policies should define procedures for:
  - Patching systems and replacing outdated devices
  - Onboarding and training employees
  - Managing visitor access
  - Addressing insider threats
  - Maintaining a safe, professional workplace



Patching Internet Facing Vulnerabilities

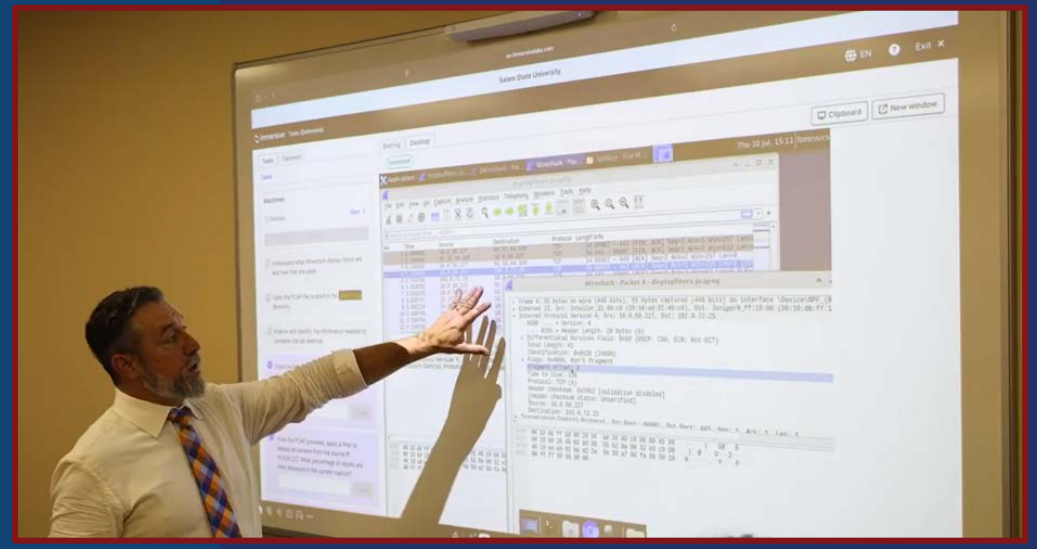
Regularly patch devices and software, including firewalls.

- 7 percent of remediations identified firewall updates as an important preventive measure.
- Prioritize updates when zero-day vulnerabilities emerge.
- Maintain continuous vulnerability monitoring to reduce exposure by signing up for Massachusetts Cybersecurity Program.

Assessments

Assess first to focus cybersecurity investments.

- Assessments identify current vulnerabilities and gaps.
- Findings help prioritize limited resources across technology and policy improvements.
- A baseline assessment is an essential first step when upgrading cybersecurity or IT systems.



Replace Legacy IT

Retire legacy IT before it becomes an attacker’s entry point.

- Legacy IT includes end-of-life hardware or software no longer supported by its vendor.
- Unsupported systems do not receive security updates or vulnerability patches.
- Risk increases over time, creating attractive entry points for attackers.

Together, We can Reduce the Risks

Recommendations based on practical remediations:

- 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.
- Replacing legacy IT.

mass.gov/consumer
masscybercenter.org

Get the full Data Breach report!
Scan the QR Code:

"Building a Cyber-Strong Massachusetts"

Visit MassCyberCenter.org to learn more.