Lauren Zabierek

Co-Founder & CEO, Software Safety Institute (SSI, currently launching)
Senior Advisor, CAS Strategies | Founder, LZX Consulting
Former Senior Advisor, CISA — Co-lead, Secure by Design Initiative
Former Executive Director, Cyber Project, Harvard Kennedy School Belfer Center

---

To: Undersecretary, Office of Consumer Affairs and Business Regulation
CEO, MassCyberCenter at the MassTech Collaborative

From: Lauren Zabierek

Re: Response to *Examining the Impact of Data Breaches in Massachusetts* (May 12, 2026)

I read with great interest your joint report “Examining the Impact of Data Breaches in Massachusetts,” released May 12, 2026. I applaud your efforts to examine data in your holdings in order to surface patterns, and believe this is an activity worth pursuing on a regular basis. I encourage you to establish mechanisms for institutional learning from this data and to develop policies that take those lessons to scale in order to prevent failures across the Commonwealth.

I write in a dual capacity: as a Massachusetts resident with a direct stake in the safety of this data, and as a practitioner with twenty-three years in the national security domain across the military, intelligence community, private sector, and academia, including co-leading the Secure by Design initiative at CISA under then-Director Jen Easterly. I am currently launching the Software Safety Institute, a nonprofit dedicated to continuing and expanding that work.

What follows are substantive suggestions that I believe could make this analysis significantly more powerful and could actually reduce the burden of cyber safety on the most vulnerable and least-resourced entities in the Commonwealth, while increasing safety for all Massachusetts residents.

1. The People-Process-Technology Lens Places the Burden in the Wrong Place

While the report evaluates its findings through a people-process-technology lens, that framework inadvertently continues a cycle of harm by placing too much responsibility on the users of software products. In reality, software companies could make their products far more secure, and they know how to. The reason they often don't is not indifference, but incentive: the market rewards speed and features, not security. Every remediation recommendation in the report, such as stronger passwords, MFA adoption, employee training, and firewall updates places the burden of action on the breached organization. The software vendors whose insecure products created the attack surface are entirely absent from the analysis.

Massachusetts has concrete mechanisms to change this dynamic. The Commonwealth's Operational Services Division IT Statewide Contracts, and the IT Vendor Terms established by EOTSS, could be updated to reflect Secure by Design principles and standardize language that strengthens the demand for security in procured products. This includes requirements such as MFA enabled by default, no default passwords, and logging included at no extra cost all of which are outlined in CISA's Secure by Demand guidance. Rather than spending scarce resources on cyber awareness training that has not moved the needle on systemic security, Massachusetts could begin to create a real market for product security and lead the nation in doing so.

2. Every Threat Vector Has Upstream Roots in Software Design

Of the 1,526 breaches analyzed, your data shows 938 system intrusions, 727 internet-facing vulnerabilities, 254 cases of human negligence, 249 third-party vectors, 245 identity-based attacks, and 207 social engineering attacks. We would argue that each of these threat vectors has root causes in software design and development, including the ones that appear on the surface to be human failures. Clicking on a phishing link is a *proximate* cause, not a root cause. Truly safe and resilient systems should be able to continue operating even in the event of inevitable human error because human error is not an anomaly, it is a constant. The more productive questions to ask of this data are: Why was one click sufficient to cause a breach? Why were unsafe defaults permitted? Why did the system lack compensating controls that would have contained the failure?

The same can be applied to the report's remediation framing. Passwords were the largest remediation category at 32 percent, but 'use stronger passwords and change them frequently' is not the modern safety answer; instead we should demand phishing-resistant MFA, passkeys, SSO availability, secure defaults, least privilege, robust logging, session controls, and eliminating password dependence wherever possible. **These are elements of safe software design, not user behavior, and ones that Massachusetts could require in their contracts.**

The internet-facing vulnerabilities that comprise the bulk of the intrusion vectors can be eliminated by design. Many of these weaknesses almost certainly appear on MITRE's Top 25 Most Dangerous Software Weaknesses and on MITRE's 2007 list of Unforgivable Vulnerabilities. These lists contain classes of defects that the software development community has known how to prevent for decades. Buffer overflows, SQL injection, and directory traversal vulnerabilities have no place in modern production software, yet they continue to appear in breach data because vendors are not incentivized to eliminate them. I would strongly encourage you to collect and publish data on which specific vulnerability classes recur in Massachusetts breach reports, and which products those vulnerabilities were observed in. Building that dataset over time would begin to establish a public record of which products harm us, and how, which is an essential precondition for accountability.

3. ‘Unknown or Other’ is a Software Product Failure

The report notes that 'unknown or other' accounts for the majority of entity-responsibility classifications with 1,793 of 2,164 incidents. This is framed as a forensic visibility challenge, and it should become a major policy finding in its own right. At this scale, the inability to attribute breaches means that organizations broadly lack adequate logging, telemetry, auditability, and the incident reconstruction capability needed to understand what happened to them. Without diagnosability, the Commonwealth cannot learn from failures or hold the right parties accountable. This is not primarily an organizational maturity problem. It is a product design problem: software vendors that do not ship with default-on logging, machine-readable audit trails, or anomaly detection are making attribution impossible for the organizations that deploy their products and for the regulators attempting to understand harm. **Your own data makes the empirical case for mandatory default-on logging and audit trail requirements.** That is a regulatory recommendation this report stops just short of making.

4. Regulated Sectors Leading in Breach Counts Is an Important Signal

Financial services (316 breaches), healthcare (293), and banks (255) lead in incident counts. These are also the most heavily regulated sectors in the Commonwealth, operating under extensive federal and state compliance frameworks. That they continue to lead in breach counts is not an indictment of regulation; rather, it is a clear signal that compliance frameworks alone are not producing security outcomes.

More importantly, these sectors are among the largest purchasers of software in Massachusetts. Their breach data should be driving Secure by Demand requirements in procurement processes. A productive next step for a future report would be to map breached organizations to their software vendors and ask: which vendors' products appear repeatedly across these incidents? That question shifts the frame from 'which organizations were victimized' to 'which products are creating persistent risk.' This question alone could drive market accountability.

5. Detection Latency Is a Software Product Failure

The Days Until Discovery data is striking: trade unions averaging 168 days, entertainment 112 days, nonprofits 105 days. The report attributes this to uneven maturity in threat monitoring capabilities, which is accurate from a governance standpoint. But it is also a software security problem. Products that do not generate machine-readable logs by default, do not surface anomalies natively, and require expensive third-party security tooling to achieve basic visibility are creating detection gaps that no amount of organizational investment can fully overcome.

The MassCyberCenter's own SOC/Range Initiative which provides managed detection and response at reduced cost for local businesses is a valuable program. But it is functioning as a workaround for a market failure, subsidizing detection capability that should be built into the products these organizations are already purchasing. I would ask: what is the SOC/Range Initiative costing Massachusetts taxpayers annually? That figure represents, in concrete dollars, the cost that software vendors are offloading onto the public; these are costs that should attach to the product, not to the victim.

6. The Cost Accounting Understates the True Harm

The report estimates approximately $1,185 per breach event for credit monitoring alone, for incidents affecting fewer than 5,000 residents. This figure is the visible floor: the direct, measurable cost borne by the breached organization. However, the externalized costs are not captured; these include resident time spent responding to identity theft, downstream fraud losses, long-term credit damage, and the cumulative erosion of trust in institutions that hold sensitive data. These costs are not evenly distributed. The burden of identity theft recovery falls disproportionately on women and marginalized communities, i.e, those with less financial cushion to absorb disruptions to critical infrastructure like transportation and education, less access to legal and financial remediation resources, and less time to navigate bureaucratic recovery processes. A full social cost accounting that captures these downstream harms would paint a significantly more complete picture of who is absorbing the cost of insecure software and would strengthen the case for software liability as a policy instrument at the state level.

It is worth noting that software companies currently disclaim liability for these harms through End User License Agreements, placing the burden squarely on software users. All of the regulations in Massachusetts, and all of the associated costs such as breach notification, credit monitoring, and enforcement fall on those end users. The vendors who shipped the vulnerable products bear none of it.

Conclusion: Massachusetts Has Led This Story Before

This data is an important first step, but the story the report is painting is that “people failed,” which is the same story perpetuated by the software companies, the cybersecurity industry, and unfortunately, the entire ecosystem. But the true story (and one that your data supports) is that organizations and vendors continue to operate systems whose defaults, architecture, maintenance model, and visibility make predictable failure likely. This pattern has a historical parallel. Before federal auto safety regulation, the dominant narrative was that crashes were caused by bad drivers. The car was exonerated; the operator was blamed. It took a sustained

policy argument grounded in empirical data and focused on the product rather than the person to finally shift responsibility upstream to manufacturers. Ralph Nader made that argument.

Massachusetts was part of that story: Nader developed his thinking as a student at Harvard Law School, and the Commonwealth was among the early states to enact its own vehicle safety protections. The safety gains that followed (seatbelts, crumple zones, crash standards and more) are now so normalized that we have forgotten they were once contested.
Software is in its 1965 moment. The products are unsafe by design, the costs are externalized onto users, and the industry's preferred narrative is that the problem lies with the people operating the technology. Massachusetts has the data, the regulatory infrastructure, and the historical precedent to tell a different story.

I have authored a report outlining how the Commonwealth could take concrete steps in this direction, and I would welcome the opportunity to share it with your offices. The data you have already collected supports a much more powerful policy argument than the current report makes. I would be glad to work with MassCyberCenter and OCABR to develop that next layer of analysis.

Thank you for your consideration.

Lauren Zabierek

Co-Founder & CEO, Software Safety Institute

lauren@softwaresafety.org

About the Author

Lauren Zabierek is a Massachusetts resident and national security practitioner with twenty-three years of experience across the military, intelligence community, private sector, and academia. She co-led the Secure by Design initiative at the Cybersecurity and Infrastructure Security Agency (CISA) under then-Director Jen Easterly as Senior Advisor to the Executive Assistant Director of the Cybersecurity Division, and led the establishment of the Cyber Response and Recovery Fund. Prior to CISA, she served as Executive Director of the Cyber Project at the Harvard Kennedy School's Belfer Center. She is currently a Senior Advisor at CAS Strategies, Founder of LZX Consulting, and is launching the Software Safety Institute — a nonprofit dedicated to advancing software safety as a matter of national and economic security. She writes on these issues at Substack: Redefining National Security. Her website is https://www.laurenzabierek.com/