# Testimony in Opposition to SB 220

Matthew Erickson
SpiderOak & The Digital Privacy Alliance
before the Ohio Senate Government Oversight & Reform Committee

May 9, 2018

Dear Chair Coley, Vice Chair Uecker, Ranking Member Schiavoni, and members,

Thank you for the opportunity to offer testimony regarding SB 220. I am Matthew Erickson, Director of Client Services and Technology for SpiderOak, a company that since 2006 has had the Department of Defense as well as many critical infrastructure companies within the Fortune 500 look to us for services protecting the integrity and confidentiality of their data. I am also the Executive Director of the Digital Privacy Alliance, a group comprised of technologists, attorneys, tech companies, and everyday people interested in commonsense privacy legislation across the United States. It is from these combined backgrounds that I come to testify on Senate Bill 220.

I applaud the Ohio legislature for striving to raise cybersecurity standards for its citizens. That the government would pick this topic as an issue to address is both timely and important. It is certainly reasonable to say that a company that can demonstrate a lack of negligence should be protected from claims of negligence. However, this bill does not achieve the goals that it sets out to achieve, and in fact can easily provide a safe harbor to substandard cybersecurity practices. There are several critical areas where this bill does not live up to its admirable goals. First, having a written cybersecurity program is much different than having a competent cybersecurity posture within an organization. Second, the cybersecurity standards cited in this bill are much more fluid in implementation than makes sense for an all-or-nothing safe harbor. Finally, the list of frameworks cited in this bill would actively undermine a competent cybersecurity posture.

Modern information security is by necessity a tricky, difficult problem. Most corporate governance typically sees it as a cost center, something for which time and resources are to be minimized. This is in contrast to the current threat environment, in which we see nation-state actors directly working to penetrate corporate and government networks across the United States. Here, we do not expect paperwork stating compliance with a policy to actively deter attackers, but instead we must reward continual, demonstrable, competent implementation of a computer security program from every business that is entrusted with the personal data of everyday people. The first failing of this bill is that it does not go far enough to ensure a company is actively doing everything it can to competently prevent data breaches before it is handed a reward. We must have continually audited proof of comprehensive compliance with recognized cybersecurity frameworks before we can reward. We must also have better means to ensure that negligence in carrying out a cybersecurity program (such as by Equifax) is not granted safe harbor.

Following that point, modern cybersecurity frameworks are by necessity flexible in implementation and design. A small neighborhood pizza joint might not have the same level of security requirements as a multinational bank or large hospital system, and modern frameworks take this into account. NIST FIPS 199 defines the needs of a security program as the highest needs from the three of integrity, confidentiality, and accessibility. This neatly provides necessary scoping for an information security program based on the actual needs around data, and not the size of the organization- if that neighborhood pizza joint is storing your credit card information and home addresses, that information is just as damaging if breached from that pizza joint as it would be from Target. The harm caused by a data breach is a property of the data itself, and not the size of the organization or its resources. In granting legal protections, this bill does not address potential mismatches between how a company perceives the value of the data it holds versus how a victim of a data breach experiences it. It is certainly possible to claim compliance with the letter of a standard without meeting the spirit of the standard, but we must hold companies to the spirit if we are to categorically disprove negligence.

Finally, this bill's selection of standards and government regulations is critically faulty. I will begin with the biggest issues: HIPAA and Gramm-Leach-Bliley are not cybersecurity standards and should not be treated as such. Hospitals are notorious for having poor cybersecurity, and, given their responsibilities to their patients, they should be held to the highest of standards instead of being given a free pass. On the website databreaches.net, out of 17,066 posts, 5,040 were concerned with health data, making it the largest single segment of breaches tracked.

Additionally, the Security Rule of HIPAA only covers "Electronic Protected Health Information", and not any other segments of the business. Should a hospital be held liability-free for its HR data just because it is required to store its Protected Health Information safely? Additionally, the other choices of standards listed in the bill seem haphazard in their inclusion. FedRAMP, for example, is a program to standardize how government agencies ensure compliance with NIST SP 800-53 when using cloud vendors, and itself is not a security standard. NIST 800-53, while an admirable goal, is specifically directed at Federal agencies and does not take the needs of private business into account. NIST SP 800-171 governs control of Federal Controlled Unclassified Information on non-Federal systems. The Federal Information Security Modernization Act of 2014 is not a cybersecurity standard in the least, but a law organizing and directing the US Federal Government's cybersecurity posture. Finally, I must ask, if one standard begins to "lag" behind the others in the eyes of the cybersecurity community, or is realistically inappropriate for a given business, what recourse does one have under this bill to address that issue?

It is in my professional view the best way to reduce risk to the businesses and people of Ohio due to data breaches is through meaningful, competent application of security standards that reduce data breaches, and not by providing protections to businesses that provide no meaningful protections to people. Thank you for your time and the opportunity to speak on this important matter.