Pennsylvania Bar Association
Cybersecurity and Data Privacy Committee
(http://cyber.pabar.org/)

An Approach to Discharging the Duty of “Reasonable Care” in Data Breach Matters

PBA Cybersecurity and Data Privacy (http://cyber.pabar.org/index.php/author/pba/) Cybersecurity (http://cyber.pabar.org/index.php/category/cybersecurity/), Data Breach (http://cyber.pabar.org/index.php/category/data-breach/) January 21, 2020

By Joseph Decker and Brett Creasy, CCE, CISSP, bit-x-bit LLC (https://www.bit-x-bit.com/index.aspx)

When a company is targeted and a data breach results, the exposure can be staggering. To take the most extreme example, Equifax’s Jan. 13, 2020 settlement of a 2017 class action data breach lawsuit, regarding a breach incident that affected approximately 147 million people, involves payments of potentially $380,500,000 into a fund for credit monitoring, plus an additional $125,000,000 for out of pocket losses, and potentially $2 billion more if all class members sign up for the monitoring. That is the largest class action data breach settlement to date. What did Equifax allegedly do wrong? According to news reports, Equifax delayed for two months in patching a known vulnerability in one of its website tools, a vulnerability that was used by hackers to exfiltrate the consumers’ data.

In July 2019, Capital One was sued by a putative class, alleging that Capital One failed to exercise reasonable care in securing and safeguarding consumers’ sensitive personal information, misconfigured its firewall, and failed to take “adequate and reasonable measures to ensure its data systems were protected.” What did Capital One allegedly do wrong? Capital One allegedly failed to properly configure a firewall.

Plaintiffs in the Capital One suit asserted common law legal theories which are typical of data breach lawsuits: breach of contract; negligence — duty to exercise reasonable care; negligence *per se* based on FTC Section 5, as interpreted, prohibiting failure to adequately protect PII.

But is it fair for companies to face huge exposures if they fail to protect what cybersecurity experts acknowledge as “unprotectable?” Experts appear to agree that no one can completely secure the data in their custody, and that a data breach is not a matter of “if,” but “when.” The “standard of care” for legal purposes cannot be perfection. But companies argue that they are being held to a “perfection” standard, made worse by the fact that the reasonableness of their data security measures is judged with the benefit of 20/20 hindsight.

How does a business discharge a legal duty to take reasonable measures to safeguard its customers’ data “reasonably,” and be able to defend its reasonableness in court? One of the best ways to demonstrate “reasonableness,” is for a company to refer to the requirements of a security standard “yardstick” which defines what are “reasonable measures,” and demonstrate that it implemented those measures.

There are many security standards, some more complex than others. The sheer complexity of some of the standards may deter companies from starting the process, or from implementing the standards in an organized fashion. The National Institute of Standards and Technology (NIST) publishes numerous standards for both the government and large companies, and NIST also publishes standards for small businesses. The core NIST standards — “*identify, protect, detect, respond and recover*” — are well known, but their implementation, and the NIST guidance, can be complex.

Most companies would do well to start with a set of standards that are easier to understand and implement. One example of a comprehensive set of security controls that are simpler to understand and implement can be found in the publications of the Center for Internet Security (CIS). The CIS controls can be mapped to the NIST framework, but in easily understandable ways. For example, the CIS breaks down the 20 NIST control groups into just three implementation groups, which are designed to help businesses of different sizes evaluate where to start the journey of improving their security posture. Implementation group one (IG1) is designed for businesses that have limited resources to implement the subcontrols — your typical small business. Implementation group two (IG2) is focused on a typical mid-sized business which has moderate resources available to it, such as a full time IT person, an IT budget, etc. Implementation group three (IG3) is the final group. IG3 is geared toward mature organizations that have considerable resources available — an entire IT department, likely a separate IT security group, and the budget to back those departments up. In other words, IG3 is for the mature organizations that may be looking at the NIST CSF or ISO requirements and are just looking for a no-nonsense approach in order to be well on their way to adhering to those larger frameworks.

Not surprisingly then, the CIS controls that are recommended for IG1 start with subcontrols such as “implement a security awareness program,” “designate management personnel to support incident handling” and “encrypt mobile device data.” These are controls that any business can adopt with minimal outside help or out-of-pocket costs. A helpful tool to see what controls to focus on first, based on the implementation groups, is even supplied freely on the CIS website (https://www.cisecurity.org/controls/cis-controls-implementation-groups/).

Although no set of controls are one hundred percent effective, implementing just the first five CIS controls has been proven to stop *85%* of real-world attacks. That number jumped to *97%* once all twenty controls are implemented, making a solid argument that the company which adopts the controls as part of the organization’s security program has acted “reasonably,” thus placing it in a more defensible legal position should a data breach occur.

Joseph Decker (https://www.bit-x-bit.com/ManagementTeam.aspx) is vice president and general counsel at bit-x-bit, where he consults with clients and counsel on a wide variety of computer forensics, incident response and e-discovery matters. He also directs bit-x-bit’s use of data analytics in e-discovery, developing strategies and overseeing the implementation of data analytics.

Brett Creasy (https://www.bit-x-bit.com/ManagementTeam.aspx) is the president and director of digital forensics at bit-x-bit, where he directs the company’s overall operations in digital forensics, e-discovery, cybersecurity and incident response.

(http://cyber.pabar.org/index.php/author/pba/)

About: **PBA Cybersecurity And Data Privacy (Http://Cyber.Pabar.Org/Index.Php/Author/Pba/)**

The Pennsylvania Cybersecurity and Data Privacy Committee analyzes cybersecurity issues and educates PBA members about legal, regulatory and industry standards that preserve the confidentiality of protected information.

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

type to search

Sign Up!

Email address: Your email address

Sign up

Recent Posts

An Approach to Discharging the Duty of “Reasonable Care” in Data Breach Matters (http://cyber.pabar.org/index.php/2020/01/21/an-approach-to-discharging-the-duty-of-reasonable-care-in-data-breach-matters/)

Looking Ahead to 2020 in the US: Preparing for Changes in Privacy and Security (http://cyber.pabar.org/index.php/2019/12/20/looking-ahead-to-2020-in-the-us-preparing-for-changes-in-privacy-and-security/)

New Nevada Privacy Law Requires Attention of Businesses and Websites Nationwide (http://cyber.pabar.org/index.php/2019/10/09/new-nevada-privacy-law-requires-attention-of-businesses-and-websites-nationwide/)

California and the UK take the Lead in Securing Internet of Things (IoT) Devices (http://cyber.pabar.org/index.php/2019/09/18/california-and-the-uk-take-the-lead-in-securing-internet-of-things-iot-devices/)

A Warning to Law Firms and Litigants: Unlawful Disclosure of PHI in Litigation Can Lead to Trouble (http://cyber.pabar.org/index.php/2019/06/28/a-warning-to-law-firms-and-litigants-unlawful-disclosure-of-phi-in-litigation-can-lead-to-trouble/)

Archives

January 2020 (http://cyber.pabar.org/index.php/2020/01/)

December 2019 (http://cyber.pabar.org/index.php/2019/12/)

October 2019 (http://cyber.pabar.org/index.php/2019/10/)

September 2019 (http://cyber.pabar.org/index.php/2019/09/)

June 2019 (http://cyber.pabar.org/index.php/2019/06/)

May 2019 (http://cyber.pabar.org/index.php/2019/05/)

April 2019 (http://cyber.pabar.org/index.php/2019/04/)

March 2019 (http://cyber.pabar.org/index.php/2019/03/)

February 2019 (http://cyber.pabar.org/index.php/2019/02/)

January 2019 (http://cyber.pabar.org/index.php/2019/01/)

December 2018 (http://cyber.pabar.org/index.php/2018/12/)

November 2018 (http://cyber.pabar.org/index.php/2018/11/)

October 2018 (http://cyber.pabar.org/index.php/2018/10/)

September 2018 (http://cyber.pabar.org/index.php/2018/09/)

August 2018 (http://cyber.pabar.org/index.php/2018/08/)

July 2018 (http://cyber.pabar.org/index.php/2018/07/)

April 2018 (http://cyber.pabar.org/index.php/2018/04/)

February 2018 (http://cyber.pabar.org/index.php/2018/02/)

Categories

American Bar Association (http://cyber.pabar.org/index.php/category/american-bar-association/)

Articles (http://cyber.pabar.org/index.php/category/articles/)

Biometric Features (http://cyber.pabar.org/index.php/category/biometric-features/)

Board Guidance (http://cyber.pabar.org/index.php/category/board-guidance/)

Constitutional law (http://cyber.pabar.org/index.php/category/constitutional-law/)

Cyber Insurance (http://cyber.pabar.org/index.php/category/cyber-insurance/)

Cyber Liability (http://cyber.pabar.org/index.php/category/cyber-liability/)

Cyber Subrogation (http://cyber.pabar.org/index.php/category/cyber-subrogation/)

Cybersecurity (http://cyber.pabar.org/index.php/category/cybersecurity/)

Data Breach (http://cyber.pabar.org/index.php/category/data-breach/)

Data Privacy (http://cyber.pabar.org/index.php/category/data-privacy/)

Ethics (http://cyber.pabar.org/index.php/category/ethics/)

GDPR Compliance (http://cyber.pabar.org/index.php/category/regulatory-compliance/gdpr-compliance/)

Guidance and Legislation (http://cyber.pabar.org/index.php/category/guidance-and-legislation/)

IoT Devices (http://cyber.pabar.org/index.php/category/iot-devices/)

National Cyber Security Centre (http://cyber.pabar.org/index.php/category/regulatory-compliance/national-cyber-security-centre/)

Pennsylvania Supreme Court (http://cyber.pabar.org/index.php/category/pennsylvania-supreme-court/)

Personal Devices (http://cyber.pabar.org/index.php/category/personal-devices/)

Protected Health Information (http://cyber.pabar.org/index.php/category/protected-health-information/)

Recent Cases (http://cyber.pabar.org/index.php/category/recent-cases/)

Regulatory Compliance (http://cyber.pabar.org/index.php/category/regulatory-compliance/)

Securities and Exchange Commission (http://cyber.pabar.org/index.php/category/securities-and-exchange-commission/)

Home (http://cyber.pabar.org/)

About (http://cyber.pabar.org/index.php/about/)

Legal Disclaimer (http://cyber.pabar.org/index.php/legal-disclaimer/)

(https://www.facebook.com (https://twitter.com (https://www.linkedin.com bar-associatio trk=NUS-body-company name)