IADC COMMITTEE NEWSLETTER

PRODUCT LIABILITY

AUGUST 2015

IN THIS ISSUE

Massive data breaches are occurring regularly at retailers, banks, mega-corporations, and government agencies, causing corporate executives and government agency directors to lose their jobs. It is only a matter of time before the courts start holding security software vendors strictly liable for the flaws and vulnerabilities in their products. Thus, in order to stay ahead in the cyberspace arms race and avoid costly lawsuits, cybersecurity companies need to employ proactive risk management tactics, as discussed further in this article.

Security Software Vendors Battle Against Impending Strict Products Liability

ABOUT THE AUTHORS

Donna L. Burden is a founding member of the law firm of Burden, Gulisano & Hansen, LLC and has over 25 years of experience as a trial attorney defending catastrophic personal injury cases primarily in the areas of trucking and transportation negligence, products liability, municipal law, as well as labor law and premises liability. Ms. Burden is also the coordinator of the firm's Emergency Response Team, which is a team of attorneys, field adjusters, accident reconstruction experts and other professionals available on a 24/7 basis to represent trucking and transportation industry clients whose vehicles have been involved in accidents across New York State. She can be reached at dlb@bghattorneys.com.

Hilarie L. Henry is an associate with the law firm of Burden, Gulisano & Hansen, LLC. She is a litigation attorney specializing in the defense of personal injury cases, primarily in the areas of trucking and automobile accidents, products liability, premises liability, and municipal law. She can be reached at hlh@bghattorneys.com.

ABOUT THE COMMITTEE

The Product Liability Committee serves all members who defend manufacturers, product sellers and product designers. Committee members publish newsletters and *Journal* articles and present educational seminars for the IADC membership at large and mini-seminars for the committee membership. Opportunities for networking and business referral are plentiful. With one listserv message post, members can obtain information on experts from the entire Committee membership. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Moses Kim
Vice Chair of Newsletter
Insley and Race, LLC
mkim@insleyrace.com

Today's Cybersecurity Arms Race Between Security Vendors and Hackers

In today's technology-centered society a massive hacking attack occurs regularly at retailers, banks, mega-corporations, and government agencies, resulting in devastating data breaches, where customers' or employees' personally identifiable information is stolen. Yet, for years, security software vendors have offered products, such as antivirus, encryption, firewall, and spyware removal software, aimed at preventing such attacks and improving financial transaction security. Despite these cybersecurity products, it seems hackers are winning the arms race against software security vendors. According to Peter Cohan, a startup economy expert, "The security problem is a hard one – adversaries are sophisticated and patient, and are continually evolving the threats they launch to stay ahead of the technology being created to stop them."[1]

Cybersecurity data breaches are omnipresent. Since 2013, when a security breach at Target compromised the private information of 110 million customers and cost the company nearly $150 million, a number of other companies, including Home Depot, Staples, PF Chang's, Neiman Marcus, Michaels, UPS, Jimmy John's, JPMorgan Chase, Sony, and many others have suffered breaches aimed at stealing shoppers' information.[2] Hackers then turn around and sell the stolen information on the black market to card counterfeiters, who paste the stolen magnetic stripes (magstripes, which hold a person's account number, expiration date, and secret CVV code) on the back of customers' credit cards onto fake credit cards using their own magstripe encoding machine.[3] Between 2005 and June 9, 2015, 5,377 data breaches were reported, involving more than 786 million estimated records.[4] In 2014, the number of U.S. data breaches hit a record high of 783, with at least 85,611,528 records exposed.[5] It does not appear these numbers will be declining anytime soon. As of July 21, 2015, the Identity Theft Resource Center reports there have been 436 data breaches in 2015, with at least 135,145,808 records exposed.[6]

---

[1] Peter Cohan, *Security Startups Challenge IBM*, FORBES, Apr. 10, 2015, *available at* http://www.forbes.com/sites/petercohan/2015/04/10/security-startups-challenge-ibm/.

[2] Tom DiChristopher, *Data Breaches Now Industrywide Problem: Target CEO*, CNBC (Nov. 28, 2014, 11:08 AM), http://www.cnbc.com/id/102220981; Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015, 7:06 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

[3] Natasha Bertrand, *Here's What Happened to Your Target Data That Was Hacked*, BUSINESS INSIDER (Oct. 20, 2014), http://www.businessinsider.com/heres-what-happened-to-your-target-data-that-was-hacked-2014-10.

[4] *Data Breaches*, IDENTITY THEFT RESOURCE CENTER, http://www.idtheftcenter.org/id-theft/data-breaches.html (last updated June 9, 2015).

[5] *Data Bre$ch Reports*, IDENTITY THEFT RESOURCE CENTER, Dec. 31, 2014, *available at* http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf (defining a data breach as "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure").

[6] *Data Breach Reports*, IDENTITY THEFT RESOURCE CENTER, July 21, 2015, *available at* http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

Corporate executives are required to certify that their computer systems are secure, risking hefty fines and long prison sentences if they are incorrect,[7] but there is currently no obligation placed on the vendors of the software used on those computer systems to certify that their products are secure.[8] In addition, *known* security vulnerabilities often remain unfixed.[9] As a result, many cybersecurity commentators are pushing for software security vendors to be held strictly liable, reasoning that in order to improve cybersecurity, security software flaws or vulnerabilities need to affect a vendor's bottom line.[10] The security software industry has rapidly evolved and matured to the point where many believe that it no longer seems unreasonable or unfair to hold security software vendors liable for defects to the same degree other product designers are held responsible for their products.[11]

Strict Product Liability for Software Developers Is on the Horizon

To date, there are no reported decisions in the U.S. holding a security software vendor liable for data breaches enabled by flawed software under a strict products liability theory.[12] However, "liability law changes with the times"[13] and more and more cases foretell such a possible legal future for security software designers.[14] On April 20, 2015, two taxpayers filed a federal lawsuit against Intuit Inc. alleging that the company's inadequate security protections in TurboTax software facilitated the filing of fraudulent tax returns.[15] Similarly, on March 24, 2014, Trustmark National Bank and Green Bank, the

[7] Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act, 15 U.S.C. §§ 7201-7266 (Supp. IV 2001-2005).

[8] Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 429 (2008).

[9] *Identity Theft Resource Center Breach Report Hits Record High in 2014*, IDENTITY THEFT RESOURCE CENTER, Jan. 12, 2015, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html ("The FBI estimates that more than 1,000 retailers are under assault with the same (or tweaked versions) of the malware that compromised Target and Home Depot.").

[10] *E.g.* Bruce Schneier, *Liability and Security*, CRYPTO-GRAM NEWSLETTER, Apr. 15, 2002, https://www.schneier.com/crypto-gram/archives/2002/0415.html#6.

[11] *Id.*

[12] *See* Daniel M. White, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 FORDHAM L. REV. 369, 385 (2011).

[13] T. Randolph Beard, PhD et al., *Tort Liability for Software Developers: A Law & Economics Perspective*, 26 J. MARSHALL J. COMPUTER & INFO. L. 199, 207 (2009).

[14] *See, e.g.,* Complaint, Diaz v. Intuit, Inc., No. 15-cv-01778 (N.D. Cal. Apr. 20, 2015); Complaint, Trustmark Nat'l Bank v. Target Corp., No. 14-CV-2069 (N.D. Ill. Mar. 24 2014); Complaint, Rice v. INSYNC, No. 30-2014-00701147-CU-NP-CJC (Cal. Super. Ct. Jan. 27, 2014); Complaint, Hamilton v. Microsoft Corp., No. BC303321 (Cal. Super. Ct. Sept. 30, 2003) (a potential class-action lawsuit calling on the courts to force Microsoft to adequately address its security problems); Complaint, Goldblatt v. Hewlett-Packard Company, No. 11-cv-05779-LHK (N.D. Cal. Dec. 1, 2011) (a potential class action-lawsuit alleging that Hewlett-Packard's printers had a software design defect that allowed hackers to install malicious updates without detection to gain access to the printer's network and steal sensitive information); *but see* Stipulation of Voluntary Dismissal, *Goldblatt*, No. 11-cv-057799-LHK (N.D. Cal. July 10, 2012).

[15] Complaint, *Diaz*, *supra* note 14, ¶ 48 ("Rather than protecting customers' personal and financial information by implementing stricter security measures, TurboTax . . . instead knowingly facilitated identity theft tax refund fraud by allowing

banks that absorbed the costs for fraudulent charges on stolen credit cards and reissuing new cards to cardholders that were victimized by the massive Target data breach, sued Target and credit card security firm Trustwave.[16] The complaint alleged that Trustwave negligently assessed Target's security and failed to adequately monitor Target's computer systems, allowing hackers to steal 40 million payment card records and encrypted PINs and 70 million customer information records containing customer information.[17] Regardless of the fact that Trustwave did not actually monitor Target's network or process its cardholder data and the banks dismissed their cases without prejudice to re-filing,[18] this lawsuit along with the Intuit lawsuit foretell the possibility of future liability for security software vendors, not only to their clients, but to the general public, as well. As more lawyers attempt to demonstrate that security software companies are contributing to the cybersecurity problem, juries may demand the companies be held accountable. But, there are several issues with applying a strict products liability theory to security software.

Product or Service

Determining whether security software is a product (product liability could apply) or a service (product liability cannot be applied) will depend upon the particular software. The *Third Restatement* defines a product as "tangible personal property distributed commercially for use or consumption"[19] and comments that "in every instance it is for the court to determine as a matter of law whether something is, or is not, a product."[20] In *Winter v. G.P. Putnam's Sons*, the Ninth Circuit in *dicta* stated that "computer software that fails to yield the result for which it was designed may be another," meaning another product, and thus, subject to strict product liability.[21] While most security software is now mass-marketed, and therefore considered a product for product liability purposes, it remains to be seen whether security software purchased by giant corporations (such as Target) is considered custom software, where there is room to negotiate the contract terms, triggering the product/service dichotomy.[22] When the definition of "product" does not provide a clear answer for the court, the determination is reached in accordance with the public policies behind strict liability, such as:

cybercriminals easy access to its customers' most private information.").

[16] Complaint, *Trustmark*, *supra* note 14.

[17] *Id.* ¶¶ 82, 84.

[18] Jonathan Stempel, *Banks Pull out of Lawsuit vs Target, Trustwave over Data Breach*, REUTERS (April 1, 2014, 12:00 PM), http://www.reuters.com/article/2014/04/01/target-trustwave-lawsuit-idUSL1N0MT0W920140401.

[19] RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 19(a) (1998) [hereinafter THIRD RESTATEMENT].

[20] *Id.* cmt. a.

[21] 938 F.2d 1033, 1036 (9th Cir. 1991) (mushroom enthusiasts who relied on erroneous information in encyclopedia of mushrooms had not strict products liability claim against publisher when they became ill).

[22] Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1581 (2005) ("Network security software is frequently a hybrid of sales and services.").

> (3) the justice of imposing the loss on the manufacturer who created the risk and reaped the profit; (4) the superior ability of the commercial enterprise to distribute the risk of injury as a cost of doing business; (5) the disparity in position and bargaining power that forces the consumer to depend entirely on the manufacturer; (6) the difficulty in requiring the injured party to trace back along the channel of trade to the source of the defect in order to prove negligence; and (7) whether the product is in the stream of commerce.[23]

These factors strongly hint that security software for corporate computer systems, such as Target, Home Depot, etc., should be considered a product for product liability purposes.[24]

Difficulties with Proving Reasonable Alternative Design

Even if software were considered a "product" allowing strict product liability to attach, plaintiffs would struggle to prove design defect. According to the *Third Restatement*, a product:

> is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe; . . . .[25]

It would be extremely difficult for a plaintiff to show a reasonable alternative design that the security software vendor should have used. This would require the plaintiff to hire an expensive technology expert to pinpoint the source of the infection in court. In 2003, Marcy Levitas Hamilton filed a class action suit against Microsoft blaming it for an intrusion by a hacker who stole and used her personal data and social security number, damaging her financial accounts and holdings.[26] This case was settled confidentially.[27] But, if it had proceeded under a products liability theory, and the plaintiff had to prove a design defect, "[g]iven the complexity of building an operating system, showing a reasonable alternative to the court—in other words, designing a new operating system—would be a near impossible task."[28] This seems to go hand in hand with attempting to formulate an alternative security software code, error-checking technique, software logic, equipment/software interface device, and/or warning provided to the operator on the screen.

[23] THIRD RESTATEMENT, *supra* note 19, Reporter's Notes to cmt. a.
[24] *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 467 (2008).
[25] THIRD RESTATEMENT, *supra* note 19, § 2(b).
[26] Complaint, *Hamilton*, *supra* note 14.
[27] Emily Kuwahara, Note, *Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers for Its Security Flaws?*, 80 S. CAL. L. REV. 997, 998 (2007).
[28] *Id.* at 1024.

Economic Loss Rule

Even if a plaintiff could prove that the security software was defectively designed, tort liability does not consider economic damage a sufficient basis for liability. Instead, economic loss claims are pursued under contractual remedies, controlled by express and implied warranties and/or End User License Agreements that require the customer to sign away his/her right to sue the software vendors for security flaws that leave his/her computers open to attack by malware. However, the ultimate victims affected (those whose personal financial information is stolen and the banks, who are forced to refund the fraudulent charges to victims[29]) are not party to the sale of the software that is used at the retail stores and have no ability to negotiate the allocation of liability if something should go wrong with the software. Even the corporations who purchase the security software are most likely unable to evaluate the quality of the product, as most cannot understand or read code. Thus, counsel for the plaintiff will argue that this burden should fall to the security software vendor to create a quality product in the first instance.

The economic loss rule is a judicially created principle that precludes parties from pursuing tort actions for purely economic or commercial losses.[30] But, economic damage is the primary type of harm caused by security software vulnerabilities, which for security software customers includes the cost of hiring IT professionals to restore the integrity of the compromised computer network, the financial harm caused by the unauthorized disclosure of sensitive data, such as having to supply identity theft protection to all victims, and the cost of replacing the faulty security software programs and licensing alternative more secure applications.[31] Banks are also left paying for fraudulent charges and for re-issuing new payment cards to victims. Yet, most courts do not allow purely economic damage claims to proceed in products liability cases.[32] While, the individual whose information was stolen may also endure

[29] *See* Regulation E, 12 C.F.R. § 1005 (protecting consumers when they use electronic fund transfers, including debit and credit payments at the point of sale, from fraudulent charges).

[30] *See* Avazpour Networking Services, Inc. v. Falconstor Software, Inc., 937 F. Supp. 2d 355 (E.D.N.Y. 2013) (dismissing plaintiff's tort actions against a software vendor for damages allegedly caused during vendor's upgrade of plaintiff's network due to economic loss doctrine and the lack of a separate and independent duty); Shema Kolainu–Hear Our Voices v. ProviderSoft, LLC, 832 F. Supp. 2d 194, 205 (E.D.N.Y. 2010) (barring plaintiff's strict liability claim for defective billing software due to economic loss rule); NMP Corp. v. Parametric Tech. Corp., 958 F. Supp. 1536, 1546-47 (N.D. Okla. 1997) (rejecting software manufacturer liability based on the economic loss rule).

[31] Liis Vihul, *The Liability of Software Manufacturers for Defective Products*, 1 THE TALLINN PAPERS: A NATO CCD COE PUBLICATION ON STRATEGIC CYBER SECURITY 1, 10 (2014), *available at* https://ccdcoe.org/publications/TP_Vol1No2_Vihul.pdf.

[32] Lori A. Weber, *Bad Bytes: The Application of Strict Products Liability to Computer Software*, 66 ST. JOHN'S L. REV. 469, 476-77 (Spring 1999) ("Strict product liability for software sold in a defective or unreasonably dangerous condition may be imposed upon a seller or manufacturer, but only if the software reached the consumer without substantial change, the consumer used the software in a reasonable fashion, and personal injury or property damage was actually caused by the software.").

economic losses,[33] the damage caused to one's identity, credit, and financial reputation is less easy to categorize. On the other hand, the Computer Fraud and Abuse Act[34] defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[35] Therefore, it is possible an exception to the economic loss rule could be created allowing victims to recover for data theft caused by a security flaw.[36] Even if this were the case, a data breach victim's economic loss would most likely be too small to encourage the victim to undertake an expensive lawsuit against the security software vendor.

Innovation and Cost Concerns

If strict products liability claims are allowed against security software vendors, such companies would be compelled to guarantee the safety of their programs. Many commentators claim this would increase security software vendors' exposure to liability, leading to the increase of insurance premiums, and resulting in costlier security software, and inhibiting innovation in the security software world.[37] They argue that if security developers cannot meet the potential security requirements the courts develop, products liability exposure could jeopardize their ability to stay in business. However, the security software manufacturing industry is a multi-billion dollar industry dominated by security startups, who are quickly earning billions, such as FireEye and Palo Alto Networks,[38] and can likely withstand such exposure. In fact, two security software companies, WhiteHat and FireEye, recently announced product liability protection for their customers in the wake of a data breach.[39]

[33] *See* Complaint at ¶¶ 47-51, Curry v. AvMed, Inc., No. 10-cv-24513-JLK (S.D. Fla. Apr. 25, 2011) (alleging the following damages from a data breach at a health insurer's corporate offices: being forced to spend money to place alerts with various credit reporting companies and contest the fraudulent charges, e.g., cellular minutes, postage, and travel-related costs; spending money for a subscription to an identity theft protection service; and losing wages to spend time meeting with the police to report and attempt to remedy the effects of identity theft).

[34] 18 U.S.C. § 1030(a)(5) (2008) (criminalizing knowingly transmitting code that "intentionally causes damages without authorization" and intentionally accessing a computer without authorization causing damage).

[35] *Id.* § 1030(e)(8).

[36] Kuwahara, *supra* note 27, at 1030.

[37] *E.g.* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE, at 215-16 (2008); Weber, *supra* note 32, at 479.

[38] *See* Rick Gordon, *The Cyber Security Market is Hot! Here's Why*, DARK READING (May 8, 2014, 12:30 PM), http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128.

[39] Kelly Jackson Higgins, *Security Product Liability Protections Emerge*, DARK READING (May 4, 2015, 5:15 PM), http://www.darkreading.com/vulnerabilities---threats/security-product-liability-protections-emerge/d/d-id/1320274 ("WhiteHat has enhanced its full-refund warranty guarantee policy for its Sentinel Elite Web vulnerability assessment service by doubling breach loss coverage to $500,000. FireEye, meantime, has obtained US Department of Homeland Security certification of its Multi-Vector Virtual Execution engine and its Dynamic Threat Intelligence cloud offering under the agency's SAFETY Act program, which protects its customers from lawsuits and other litigation in the wake of a major cyberattack.").

Unpredictability and Complexity of Cybersecurity

Strict product liability for security software is problematic because "many future security needs cannot be predicted with any certainty, posing a difficult challenge for designers."[40] Vendor liability would unjustifiably punish the developers who are trying to help customers protect their systems when hackers are the true culprits. Hence, some argue that security software developers should face liability for damage resulting from *avoidable* security flaws exploited to infect a user with malware. This would again require an expert to pinpoint the source of the infection and a "definition of what flaws are avoidable informed by legal precedence from earlier cases,"[41] which are currently nonexistent. In addition, security software designers should not be held liable for "inadvertent or intentional acts by insiders with access to a system, supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day,[42] vulnerabilities with no established fix."[43]

Commentators argue that it is good policy to place the burden on the software security developers because they are in the best position to understand potential product defects and accordingly, alter the risk of any security breaches.[44] However, both the security software vendor and *its customer* need to exercise care in order to decrease the probability of a data breach. Thus, the interplay and cooperation between the two parties makes it difficult to hold the security software vendor strictly liable, especially when the customer is the one who needs to install patches or updates to the software.

Risk Management Advice for Security Software Vendors and Their Defense Counsel

Whether or not the courts will hold security software vendors strictly liable for their security flaws and vulnerabilities remains to be seen. In the meantime, defense counsel should encourage its cybersecurity clientele to employ proactive risk management tactics that will keep them ahead in the cyberspace arms race and help them avoid costly lawsuits. More specifically, vendors should employ a "rigorous process to identify and address

[40] Eric A. Fisher, Senior Specialist in Sci. and Tech. Cong. Research Serv., Statement before the Subcommittee on Research and Technology Committee on Science, Space, and Technology U.S. House of Representatives, The Expanding Cyber Threat, Jan. 27, 2015, *available at* http://docs.house.gov/meetings/SY/SY15/20150127/102902/HHRG-114-SY15-Wstate-FischerE-20150127.pdf.

[41] Nick Heath, *Should Developers Be Sued for Security Holes?*, TECHREPUBLIC UK (Aug. 23, 2013, 12:42 AM), http://www.techrepublic.com/blog/european-technology/should-developers-be-sued-for-security-holes/.

[42] A "zero-day" attack is defined as "an exploit, worm or a virus capable of crippling global web infrastructure either prior to, or within hours of, a public announcement of a computer system vulnerability." Siobhan McBride, *Zero Day Attack Imminent*, COMPUTERWORLD (Feb. 28, 2005, 8:08 AM), http://www.computerworld.com.au/article/1535/zero_day_attack_imminent/.

[43] Fisher, *supra* note 40.

[44] *E.g.* Beard, *supra* note 13, at 207.

threats and vulnerabilities, design[] software and hardware controls to address these vulnerabilities, build[] time in the testing process to assure the quality and effectiveness of controls and develop[] documentation of the efforts."[45] Vendors should also review the CWE/SANS Top 25 Most Dangerous Software Errors,[46] a catalogue developed jointly by software security experts and corporations detailing 25 common, highly dangerous software vulnerabilities, to ensure their software does not contain any of these avoidable errors. In addition, the software and all of its controls should be tested periodically and the results reviewed to evaluate any holes and potential for harm. Any anomalies should be patched as quickly as possible. Software vendors should also purchase product liability and/or cyber insurance.

Vendors may assume some level of responsibility for data breaches in their contracts to increase their competitive edge in the security software market, but they should also aim for wording that limits those liabilities as much as possible, such as WhiteHat did by specifying liquidated damages at a certain amount for data breaches.[47] In addition, vendors may also limit a purchaser's remedies to the repair or replacement of the defective software, or to the price of the software. A vendor's contract should definitively address the responsibilities of the vendor, the installer, and the user. Depending on the type of software, the contract could specify that the customer must hire qualified operators and immediately notify the vendor of any bugs in the program after they are discovered.

Finally, security software vendors should seek Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act)[48] designation and/or certification from the Department of Homeland Security (DHS) to limit their liability for claims arising out of, relating to, or resulting from terrorism, which includes cyberattacks. If designated as a qualified anti-terrorism technology (QATT), the software developer's third-party liability is capped at a DHS predetermined level.[49] If the higher-tiered protection, certification, is obtained, the developer is entitled to utilize the "government contractor defense," an affirmative defense that completely immunizes the seller from third-party liability.[50] In April 2015, DHS *certified* its first cybersecurity products, FireEye Inc.'s Multi-Vector Virtual Execution engine and Dynamic Threat Intelligence cloud platform.[51] Designation or certification as a QATT is likely

[45] Zurich, *The Liability of Technology Companies for Data Breaches*, 8 (2010), https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf.
[46] Steve Christey, *2011 CWE/SANS Top 25 Most Dangerous Software Errors*, CWE (Sept. 13, 2011), http://cwe.mitre.org/top25/.
[47] *See supra* text accompanying note 39.
[48] 6 U.S.C. § 441-44 (2002).
[49] *Id.* § 442; 6 C.F.R. § 25.7 (2006).
[50] 6 U.S.C. § 442(d); 6 C.F.R. § 25.8 (2006); Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), 71 FR 33147-01 (June 8, 2006).
[51] Brian E. Finch & Aimee P. Ghosh, *DHS Breaks New Ground with Issuance of SAFETY Act Certifications for Advanced Cybersecurity Defense Systems*, PILLSBURY WINTHROP SHAW PITTMAN LLP, 1-2 (May 11, 2015),

to have an extremely positive effect on a cybersecurity product's market performance and mitigation of its liability risks caused by cyberattacks.

available at http://www.pillsburylaw.com/siteFiles/Publications/AlertMay2015PubPolicyDHSBreaksNewGround.pdf.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

JULY 2015
Re-Examining the Learned Intermediary Doctrine: The Age-Old Theory Appears Alive and Well
Sara M. Turner and Julie Schiff

JUNE 2015
When to Show Your Cards: Strategic Considerations for When to Use Damaging Information on Your Opponent
Cynthia Arends

Protective Orders and Discovery Sharing: Beware of Plaintiffs Bearing Sharing Agreements
Joshua K. Leader and Gloria Koo

MAY 2015
Satellite Witnesses: Can Corporate Witnesses be Required to Testify Live From Across the Country?
Sherry Knutson and Michelle Ramirez

Self-Driving Technology and Autonomous Vehicles: A Whole New World for Potential Product Liability Discussion
Roy Alan Cohen

APRIL 2015
Watts v. Medicis Pharmaceutical Corporation – Trend or Outlier? Why This Case Should Remain on the Outskirts
Tonya Newman and Valerie Raedy

Alabama Supreme Court Upholds Landmark Ruling that Brand-Name Drug Manufacturers Can be Held Liable for Injuries Caused by Generic Drugs
Carol P. Michel and Brannon J. Arnold

MARCH 2015
Comcast v. Berhrend: Was the Optimism Warranted?
Kelly Anne Luther

FEBRUARY 2015
Legal Issues for the Product Liability Blogger
Jeffrey R. Lilly and Bradley B. Bush

A Primer on Product Recalls
Scott Kozak and Casey Housley

DECEMBER 2014
Alternative Approaches to Alternative Design: Understanding the Reasonable Alternative Design Requirement and Its Different Applications
Alex Purvis and Simon Bailey

NOVEMBER 2014
Expert Testimony that Contradicts Plaintiff's Testimony is Admissible in the Sixth Circuit
Jim Doran and Jackie Garfield