Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 30 | Issue 3 Article 1

January 2013

Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act

Brian E. Finch

Leslie H. Spiegel

LITIGATION FOLLOWING A CYBER ATTACK: POSSIBLE OUTCOMES AND MITIGATION STRATEGIES UTILIZING THE SAFETY ACT

Brian E. Finch† and Leslie H. Spiegel††

Abstract

Liability for a cyber attack is not limited to the attackers. An attack may be foreseeable in some circumstances, and the failure of the target or the other entities to take steps to prevent the attack can constitute a breach of duty to injured victims. In the absence of the protections provided by the Support Anti-Terrorism By Fostering Effective Technologies (SAFETY) Act, a cyber attack on a chemical facility could give rise to a number of common-law tort and contract claims against the target of the attack and other entities, potentially including the target's cyber security vendors. This article discusses claims that might arise in various cyber attack scenarios and the effect of the SAFETY Act on these potential claims.

The SAFETY Act is a tort liability management statute that was passed as part of the Homeland Security Act of 2002. Under the SAFETY Act, entities that sell or otherwise deploy products that can be used to deter, defend against, respond to, mitigate, or otherwise combat "acts of terrorism" are eligible to receive liability protections. These liability protections can take the form of jurisdictional defenses, a cap on liability, or a presumption of immediate dismissal of third-party liability claims.

This article reviews several scenarios to examine whether liability could be found against companies that make cyber security tools or against entities that purchase such tools. The article then examines how the SAFETY Act could be utilized to mitigate or eliminate such liability.

† Brian E. Finch is a partner at Dickstein Shapiro LLP and a Professorial Lecturer of Law at The George Washington University Law School. He blogs for the Huffington Post on cyber security and has a weekly cyber security column on the Fox business network website.

†† Leslie H. Spiegel is a Senior Risk and Compliance Attorney at Dickstein Shapiro.

TABLE OF CONTENTS

INTRODUCTION

Liability for a cyber attack is not limited to the attackers. An attack may be foreseeable in some circumstances, and the failure of the target or the other entities to take steps to prevent the attack can constitute a breach of duty to injured victims. In the absence of the protections provided by the Support Anti-Terrorism By Fostering Effective Technologies (SAFETY) Act, a cyber attack on a chemical facility could give rise to a number of common-law tort and contract claims[1] against the target of the attack and other entities, potentially including the target's cyber security vendors. This article discusses claims that might arise in various cyber attack scenarios and the effect of the SAFETY Act on these potential claims.[2]

The SAFETY Act is a tort liability management statute that was passed as part of the Homeland Security Act of 2002.[3] Under the SAFETY Act, entities that sell or otherwise deploy products that can be used to deter, defend against, respond to, mitigate, or otherwise combat "acts of terrorism" are eligible to receive liability protections. These liability protections can take the form of jurisdictional defenses, a cap on liability, or a presumption of immediate dismissal of third-party liability claims.

As discussed above, this article will review several scenarios to examine whether liability could be found against companies that make cyber security tools or against entities that purchase such tools. The article will then examine how the SAFETY Act could be utilized to mitigate or eliminate such liability.

I. LIABILITY SCENARIOS FOLLOWING A CYBER ATTACK

Cyber attacks are a well-recognized threat in today's world.[4]

1. Other civil claims may also arise from a cyber attack. This article does not discuss potential claims based on the theft of personal information, claims based on state or federal environmental regulations, claims based on other statutory law, potential liability for criminal negligence, or other criminal claims including claims against the attackers themselves. *See, e.g.*, JENNIFER L. MACHLIN & TOMME R. YOUNG, MANAGING ENVIRONMENTAL RISK - REAL ESTATE AND BUSINESS TRANSACTIONS LAW § 8:21 (West ed., 2012) (discussing landowners' potential environmental liability for contamination caused by third parties' acts).

2. Of course, various common law or other defenses also may be available to these claims, and these claims might be more or less viable depending on the circumstances.

3. *See* 6 U.S.C. § 441-44 (2002).

4. *See* SENATE SELECT COMM. ON INTELLIGENCE, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (Jan. 29, 2014), *available at* http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf (statement for the record of James R. Clapper, Director of National Intelligence).

Companies are regularly subjected to breach attempts by individuals, organized crime, and even nation-states. These attacks have various motives, ranging from the theft of financial information or intellectual property to the disruption or destruction of operations, data, or physical facilities.[5] Below are several scenarios describing potential cyber attacks and an examination about the potential liability resulting from each.

A. Scenario One

A company that stores dangerous chemicals in large multi-thousand gallon tanks purchases cyber security software and hardware (physical devices attached to IT systems as a cyber security measure) to prevent outsiders from breaking into their industrial control systems. Through news reports and government-furnished intelligence, the company is well aware that, while it is not being specifically targeted by cyber-attackers, hackers have been breaking into chemical companies and seeking to take control of industrial control systems. The company has purchased "firewall" and "anti-virus" systems to protect its facilities, including the systems that control the storage tanks. Alternative cyber security systems could have been purchased that would have protected against additional types of threats. However, the company elected not to purchase such cyber security technologies. A sophisticated cyber attack then occurs. The attack was specifically designed to avoid the cyber defenses the company purchased. As a result of the attack, dangerous chemicals were released into the atmosphere, seriously injuring a number of people in a two-mile radius and even killing several people. In addition, because of the release of the chemicals, deliveries to the company's customers are delayed or cancelled, causing those customers to slow or even halt production of their products.

1. Claims Against the Chemical Company

Under the laws of various jurisdictions, the company might be liable for a variety of common law claims including negligence, strict

5. *See, e.g.*, U.S. SENATE COMM. ON COMMERCE, SCI., AND TRANSP., A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH (Mar. 26, 2014), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883; *FireEye Advanced Threat Report – 2H 2012*, FIREEYE 14-17, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf (last accessed Mar. 30, 2014); Ellen Knickmeyer, *After Cyberattacks, Saudi Steps Up Online Security*, THE WALL STREET JOURNAL (Aug. 26, 2014, 10:22 AM), http://blogs.wsj.com/middleeast/2013/08/26/after-cyberattacks-saudi-steps-up-online-security/.

liability for abnormally dangerous activities, and contract claims.

a. Negligence Claims

A plaintiff injured by the release of chemicals may allege that the storage company had an obligation to take further steps to prevent the cyber attack. The success of this claim will depend on: the foreseeability of the harm, the extent of the company's duty to the plaintiff, and the causal connection between the company's failure to act and the harm. A defendant's negligence may give rise to liability, even if a third party's criminal activity also contributed to the plaintiff's harm, if the criminal activity was foreseeable.[6]

Several cases suggest that large-scale terrorist attacks may be foreseeable in some circumstances. For example, in a 2004 decision, a New York state court rejected an argument that the 1993 bombing of the World Trade Center was unforeseeable as a matter of law.[7] The court noted that the duty of property owners and landlords who hold their land "open to the public" includes an obligation to "tak[e] minimal security precautions against reasonably foreseeable criminal acts by third parties."[8] A particular harm may be foreseeable if the landlord knew or should have known of the risk of that harm.[9]

> [A] landlord does not need to have had a past experience with the exact criminal activity, in the same place, and of the same type, before liability can be imposed for failing to take reasonable precautions to discover, warn, or protect. The inquiry focuses on what risks were reasonably to be perceived.[10]

6. *See* RESTATEMENT (SECOND) OF TORTS §§ 448, 449 (1965); Ellen M. Bublick, *Upside Down? Terrorists, Proprietors, and Civil Responsibility for Crime Prevention in the Post-9/11 Tort-Reform World*, 41 LOY. L.A. L. REV. 1483, 1511 (2008) ("[P]roperty owners are ordinarily expected to take reasonable care to protect against foreseeable crime."); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 273 (2005) (suggesting that database administrators may be liable for injury from cyber attacks, particularly when the administrators have a business relationship with the victims, because identity theft is a foreseeable result of inadequately securing data); *but cf.* Port Authority of New York and New Jersey v. Arcadian Corp., 189 F.3d 305, 318-19 (3d Cir. 1999) (finding that "the [1993] World Trade Center bombing was not a natural or probable consequence of any design defect in defendants' products").

7. *See generally In re* World Trade Center Bombing Litig., 776 N.Y.S.2d 713 (N.Y. Sup. Ct. 2004) (denying summary judgment for the Port Authority of New York and New Jersey).

8. *Id*. at 734.

9. *Id*. at 734-36 (holding that a terrorist attack was not unforeseeable as a matter of law when there was "evidence of the [building operator's] actual notice of the risk of infiltration of this kind of terrorist activity").

10. *Id*. at 735, 739 (finding that the property owner's own security analysis and other

Similarly, a federal court declined to dismiss claims against airlines and airplane manufacturers by plaintiffs injured in the September 11 attacks.[11] "In order to be considered foreseeable, the precise manner in which the harm was inflicted need not be perfectly predicted."[12] The airlines "reasonably could foresee that crashes causing death and destruction on the grounds was a hazard that would arise should hijackers take control of a plane" through inadequate security screening, even if they could not foresee the specific attacks.[13] Likewise, an airplane manufacturer might have foreseen "that a failure to design a secure cockpit could contribute to a breaking and entering into, and a take-over of, a cockpit by hijackers or other unauthorized individuals."[14]

A similar standard of care may apply to cyber attacks that result in personal injury or property damage.[15] An injured claimant would need to show that the chemical company violated its duty of reasonable care by failing to protect against a foreseeable danger.[16]

> The backside of the general rule that insulates the defendant from liability in cases of unforeseeable intervening criminal acts is that if a criminal or intentional intervening act is foreseeable, or is part of the original risk negligently created by the defendant in the first place, then the harm is not outside the scope of the defendant's liability—or as most courts still put it, the criminal or intentional act is not a superseding cause.[17]

Whether an attack was foreseeable will involve factual questions

information put it "on notice of a serious risk of infiltration of terrorist activity in the parking garage" where the attack took place).

11. *See generally In re* September 11 Litig., 280 F. Supp. 2d 279 (S.D.N.Y. 2003).

12. *Id*. at 295.

13. *Id*. at 296.

14. *Id*. at 307, 312-13.

15. *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1585 (2005) ("The owner of a website, like any other retail establishment, could theoretically be liable for the reasonably foreseeable harm caused by third parties that injure customers.").

16. *Cf*. Levy-Zentner Co. v. Southern Pac. Transportation Co., 74 Cal. App. 3d 762, 781 (Cal. Ct. App. 1977) (reasoning that a landowner could be liable for injuries from a fire possibly caused by third parties when "the [plaintiff] tenants and owners presented evidence strongly indicating that the fire danger presented by itinerants was reasonably foreseeable"); *cf*. Tyson v. Danbury Mall Ltd. P'ship., 811 N.Y.S.2d 105, 105-06 (N.Y. App. 2d 2006) (holding that a property owner and manager were not liable for injuries to a plaintiff that occurred when the plaintiff chased a suspected thief because the defendants "provided sufficient security and [] the conduct of the individual who stole the plaintiff's wallet, which gave rise to the plaintiff's injuries, was not foreseeable").

17. DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, THE LAW OF TORTS § 209 (2d ed. 2013).

related to, inter alia, the risk of the particular attack that occurred, the company's awareness of the risk, and the standard of care generally applied to companies storing dangerous chemicals.[18]

The nature of the company's duty to an injured plaintiff may also be relevant. An entity that stores or handles dangerous chemicals may have a heightened duty of care.[19] Whether the nature of the company's work gives rise to that heightened duty of care and whether or not it met that duty will depend on the circumstances. The company could be liable for negligent storage or other negligence if reasonable additional security protections would have prevented the attack.[20] Although in some circumstances the criminal act of a third party acts as a superseding cause of harm, that rule may not apply when "the [defendant] at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort of crime."[21] In that case, site operators may be held liable for harm caused to third parties by criminal intrusion on

18. *See In re September 11 Litig*., 280 F. Supp. 2d at 301 ("A finding of duty does not require a defendant to have been aware of a specific hazard. It is enough to have foreseen the risk of serious fires within the buildings and the goal of terrorists to attack the buildings."); James v. Jamie Towers Housing Co., Inc., 790 N.E.2d 1147, 1148-49 (2003) ("[B]y providing locking doors, an intercom service and 24–hour security, [a property owner] discharged its common-law duty to take minimal security precautions against reasonably foreseeable criminal acts by third parties . . . ."); *In re* World Trade Center Bombing Litig., 776 N.Y.S.2d 713 (2004) (discussing foreseeability of particular terrorist attack); *cf.* Chemical Facility Anti-Terrorism Standards, 6 C.F.R. § 27.410 (2012) ("Nothing in this part shall confer upon any person except the Secretary a right of action, in law or equity, for any remedy including, but not limited to, injunctions or damages to enforce any provision of this Part."); AMERICAN CHEMISTRY COUNSEL ET AL., SITE SECURITY GUIDELINES FOR THE U.S. CHEMICAL INDUSTRY (2001), *available at* http://www.socma.com/assets/File/socma1/PDFfiles/securityworkshop/SecurityGuideFinal10-22.pdf.

19. 59 N.Y. JUR. 2D *Explosives and Fires* § 37 ("Since the measure of care required is that which is proportionate to the danger, a person who has in his or her possession an explosive substance of a dangerous character is bound to the exercise of a high degree of care to keep and guard it so as to prevent injury to others, and such duty cannot be delegated to an independent contractor."); *see* Garza v. United States 809 F.2d 1170, 1172 (5th Cir. 1987) (noting "the elevated duty of care imposed by Texas law on those who use and handle explosives"); *see also* Mayor and Council of City of Morgan City v. Jesse J. Fontenot, Inc., 460 So. 2d 685, 687 (La. Ct. App. 1984) (noting that companies that stored and transported dangerous chemicals "were under a duty to carefully handle the combustible and/or flammable liquids in their control or possession so that an unreasonable risk of harm would not be created for others"); *see generally* Pond v. Regis, 270 N.Y.S.2d 121 (N.Y. App. Div. 1966) (noting that landowners may have a duty to a child trespasser to maintain explosives safely).

20. *See* RESTATEMENT (SECOND) OF TORTS § 448 (1965).

21. *See id.*; *see also* 14 N.Y. PRAC., NEW YORK LAW OF TORTS § 6:22 ("The chief factor in determining whether the defendant [landowner] owes a duty to a plaintiff to prevent harm from a third person is foreseeability of the risk of harm.").

their site.[22]

In this scenario, the company was "well aware of the cyberthreat," and depending on the circumstances, a finder of fact might conclude that the cyber attack and the resulting chemical release and injuries were foreseeable.[23] The company's failure to procure effective cyber security systems might then be considered a proximate cause of the plaintiffs' injuries.[24]

However, the mere fact that the company was aware of the risk of a cyber attack may not be enough to render the cyber attack foreseeable and the company liable.[25] The failure to secure the site

22. *See* Yukon Equipment, Inc. v. Fireman's Fund Ins. Co., 585 P.2d 1206, 1211 (Alaska 1978) (finding that "[t]he incendiary destruction of premises by thieves to cover evidence of theft is not so uncommon an occurrence that it can be regarded as highly extraordinary [and] the particular kind of result threatened by the defendant's conduct, the storage of explosives, was an explosion at the storage site," and so the criminal activity was not a superseding cause of injury); Randolph C. Visser et al., *Volatile Combinations*, LOS ANGELES LAWYER, Nov. 2002, at 39 ("[C]hemical companies may also have a duty to protect their sites.").

23. *See In re* September 11 Litig., 280 F. Supp. 2d 279, 301 (S.D.N.Y. 2003); RESTATEMENT (SECOND) OF TORTS § 449 (1965) ("If the likelihood that a third person may act in a particular manner is the hazard . . . which makes the actor negligent, such an act, whether innocent, negligent, intentionally tortious, or criminal does not prevent the actor from being liable for harm caused thereby."); RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 19 cmt. c (2013) ("If the third party's misconduct is among the risks making the defendant's conduct negligent, then ordinarily plaintiff's harm will be within the defendant's scope of liability."); Visser, *supra* note 22, at 42 ("[C]ourts must now determine whether the events of September 11, 2001, when combined with the 1995 Oklahoma City and 1993 World Trade Center bombings and the political trend to protect the public from potential chemical terrorism, have served to put all industries that deal in hazardous substances on notice to consider the foreseeability of their products being used in a terrorist attack."); *cf.* Levy-Zentner Co. v. Southern Pac. Transportation Co., 74 Cal. App. 3d 762, 781 (Cal. Ct. App. 1977) (noting that a fire caused by trespassers on a landowner's property may have been foreseeable).

24. *See* Doyle v. Exxon Corp., 592 F.2d 44, 48 (2d Cir. 1979) (reasoning that, under Vermont law, when a gas station owner was aware of a particular gas station's vulnerability to robbery and also of additional protections that could be put into place, "a jury could logically conclude that the criminal events at [a gas] station on the night in question resulted, at least in part, from [an owner's] failure to install in a timely fashion a system designed to prevent the very wrong that occurred, even though a contrary conclusion could rationally be based on the same evidence"); *see also Levy-Zentner Co.*, 74 Cal. App. 3d at 776 (stating that a landowner could be held negligent for losses from a fire that began in its property when among other factors it "neglected the rudiments of basic fire protection and inspection . . . and in violation of its own regulations failed to take precautions against continuing itinerant activity that had also caused [an earlier] fire").

25. *See* Order and Opinion Granting United's Motion for Summary Judgment That It Had No Duty for Flight 11, *In re* September 11 Litig., No. 21 MC 101 (AKH) (S.D.N.Y. Nov. 21, 2012) (finding that harm from terrorist attack was not reasonably foreseeable to an airline that assisted in security screening when the terrorists used another airline's planes in the attack and noting New York courts' "caution regarding the extension of liability to defendants for their failure to control the conduct of others in light of the potential for unfairness and potentially limitless liability"); District of Columbia v. Doe, 524 A.2d 30, 33 (D.C. 1987) ("[B]ecause of

properly must have negligently "created or increased the risk of harm," or the company must have had another specific duty to the injured parties.[26]

A claimant might argue that the company's failure to procure appropriate security systems "increased the risk of harm" in light of the company's knowledge that its site would be an attractive target for terrorists and that it was vulnerable to a particular type of attack.[27] Whether that argument would succeed would depend on the circumstances, including the foreseeability of the particular attack that occurred and the adequacy of the company's protections.

b. Strict Liability Claims

The company could be held strictly liable if a court concludes that the company's storage of the chemicals constituted an abnormally dangerous activity under the circumstances.[28] Courts are split on when the storage of chemicals constitutes the type of abnormally dangerous activity that can give rise to strict liability.[29] Whether the company could be held strictly liable for the discharge

---

the extraordinary nature of criminal conduct, the law requires that the foreseeability of the risk of such conduct must be 'more precisely shown' than is usually required in a typical negligence situation."); RESTATEMENT (SECOND) OF TORTS § 449 cmt. a (1965); DOBBS ET AL., *supra* note 17 ("once courts decide that a defendant should use reasonable care to protect the plaintiff from crimes, foreseeability of crime has become an issue of fact, not a rule of law. . . . [T]here is no blanket duty [to protect against criminal activity] any more than there is a blanket immunity").

26. *See* RESTATEMENT (SECOND) OF TORTS § 449 cmt. a (1965); *see also In re* September 11 Litig., 280 F. Supp. 2d 279, 290-93 (S.D.N.Y. 2003) (airlines and airport security companies owed a duty of care to victims of the September 11 attacks who did not travel on the planes used in the attack; "courts have imposed a duty when the defendant has control over the third party tortfeasor's actions, or the relationship between the defendant and plaintiff requires the defendant to protect the plaintiff from the conduct of others"); *cf.* Port Authority of New York and New Jersey v. Arcadian Corp., 189 F.3d 305, 313 (3d Cir. 1999) ("[M]anufacturers have no duty to prevent a criminal misuse of their products which is entirely foreign to the purpose for which the product was intended.").

27. *See* District of Columbia v. Doe, 524 A.2d 30, 33 (D.C. 1987) (finding a school could be held liable for the rape of a student when "school officials were on notice of the danger to students from assaultive criminal conduct by intruders"); Cross v. Wells Fargo Alarm Svcs., 412 N.E.2d 472, 474-75 (Ill. 1980) (finding a landlord could be held liable for failing to provide adequate security when a tenant was injured in a crime on the premises).

28. *See* Yukon Equipment, Inc. v. Fireman's Fund Ins. Co., 585 P.2d 1206, 1211 (Alaska 1978) ("The considerations which impel cutting off liability where there is a superseding cause in negligence cases also apply to cases of absolute liability"); DOBBS, HAYDEN & BUBLICK, *supra* note 17 ("Courts now have generally accepted the principle that for some activities involving special dangers, especially those not commonly pursued, liability can be imposed without fault."); Visser, *supra* note 22 (noting potential claims and defenses).

29. *See* DOBBS, HAYDEN & BUBLICK, *supra* note 17 (noting that courts are split on whether strict liability should be applied to "use or storage of explosives and similar activities").

under a tort theory would depend on whether the applicable laws of the jurisdiction considered the company's activities to be abnormally dangerous in light of its surroundings, the risks involved, and steps the company could take to mitigate those risks (if any).[30] In addition, many courts are reluctant to impose strict liability on companies based on injury from a third party's act.[31]

c. Contract Claims

Depending on the terms of the storage company's agreements with its customers, it might also be liable for breach of contract claims for failing to make deliveries on time. The viability of contract claims may depend in part on whether the agreements provide that terrorism is an excuse for non-performance or whether other excuses for non-performance apply.[32]

2. Claims Against Other Entities

Injured parties might assert products liability claims against the manufacturers of the chemicals or the tanks, but those claims are unlikely to be successful absent unusual circumstances.[33] Courts have rejected similar claims arising out of terrorist attacks, finding that, in most circumstances, manufacturers do not have a duty to anticipate

30. DOBBS, HAYDEN & BUBLICK, *supra* note 17 (discussing factors considered by courts); *see also* Visser, *supra* note 22, at 41.

31. *Compare* Bianchini v. Humble Pipe Line Co., 480 F.2d 251 (5th Cir. 1973) (applying Louisiana law and declining to hold a pipeline company strictly liable for harm caused by an oil leak when a ship hit the pipeline); Pecan Shoppe of Springfield, Missouri, Inc. v. Tri-State Motor Transit Co., 573 S.W.2d 431 (Mo. Ct. App. 1978) (finding a motor carrier transporting dynamite not strictly liable for harm caused to plaintiffs when a third party shot its truck and caused an explosion); *with* Yukon Equipment, Inc. v. Fireman's Fund Ins. Co., 585 P.2d 1206, 1211 (Alaska 1978). *See also* Port Authority of New York and New Jersey v. Arcadian Corp., 189 F.3d 305, 313 (3d Cir. 1999) (addressing strict liability products claims and concluding that manufacturers of products that were not inherently dangerous did not have an obligation to prevent buyers from "incorporating the [product] into another device that is or may be dangerous"); RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 34 cmt. d (2005) (noting a commentator's "instinctive recoil . . . against holding the defendant strictly liable when a third party, seeking to cause harm, deliberately . . . ignites the defendant's nitroglycerin factory"). The Third Restatement "employs a unitary standard" but "addresses the different risks posed by different heads of strict liability" while "the case law in inconsistent in how much emphasis it places on the foreseeability of the intervening act." RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 34 cmt. d (2005).

32. *See, e.g.*, 30 WILLISTON ON CONTRACTS § 77:31 (4th ed., 2004) (discussing *force majeure* clauses).

33. *See Port Authority*, 189 F.3d 305; *see also* Gaines-Tabb v. ICI Explosives, USA, Inc., 160 F. 3d 613 (10th Cir. 1998).

the criminal misuse of their products.[34]

a. Design Defect Claims

An injured plaintiff might assert that the manufacturer of the chemicals should have taken steps to decrease the risk of harm from the chemicals.[35] The fact that the chemicals could be misused by criminals is unlikely to give rise to a successful products claim against the manufacturer; the plaintiff would need to establish that the chemicals were unsafe as used by an "ordinary consumer."[36]

The plaintiff might also allege that the tank manufacturer should have designed its tanks in a more secure way.[37] Such claims could sound in strict liability, and their success would depend on the facts.[38] As a comparison, one court declined to find a builder liable for harm from the September 11 terrorist attacks when "'[t]he risk reasonably to be perceived' by [defendants], and their 'duty to be obeyed,' [in designing the building] did not encompass the strange, improbable, and attenuated chain of events that led to 7 World Trade Center's collapse" and other losses.[39]

b. Failure-to-Warn Claims

A plaintiff might also assert failure-to-warn claims against the chemical manufacturer or the tank manufacturer.[40] Those claims might assert that the chemical manufacturer should have warned of the harm from the chemicals and the importance of securing them from unauthorized access and/or that the tank manufacturer should have warned that the tanks could be vulnerable to cyber attacks unless

34. *See Port Authority*, 189 F.3d at 313; *see also Gaines-Tabb*, 160 F.3d 613; Visser, *supra* note 22 (discussing case law).

35. *See Port Authority*, 189 F.3d at 310-11 (describing allegations that the manufacturers of chemicals used in the 1993 attack on the World Trade Center should have reformulated the chemicals to "decrease or eliminate their explosive properties"); *see also Gaines-Tabb*, 160 F.3d at 624-25 (rejecting similar allegations by plaintiffs injured in the 1995 Oklahoma City bombing).

36. *See Gaines-Tabb*, 160 F.3d at 624-25.

37. *See Port Authority*, 189 F.3d at 310-11.

38. *Id*. at 312 ("[U]nder New York law, theories of negligence and strict liability for design and warning defects are functionally equivalent.").

39. *See* Aegis Ins. Services, Inc. v. 7 World Trade Co., 865 F. Supp. 2d 370, 384 (S.D.N.Y. 2011).

40. *See Port Authority*, 189 F.3d at 310-11 (describing allegations that defendant manufacturers failed to advise their distributors and customers "to confirm that buyers in the general and unrestricted public market have legitimate and lawful purposes for use of Defendant's products").

additional protections were installed.

In this scenario, however, the company storing the chemicals was aware of those particular risks. A manufacturer's failure to warn gives rise to liability only if "such a warning would have prevented the harm."[41] A court might be disinclined to find that the manufacturers were required to provide additional warnings about a potential attack.[42] Companies are unlikely to have an obligation to "warn the suppliers of its product of possible criminal misuse."[43]

B. Scenario Two

Assume for Scenario Two the same facts as Scenario One, except that the chemical company buys an industrial control system (ICS) without evaluating the security risks associated with it. The company never inquires as to whether the ICS has been successfully subjected to a cyber attack before or whether the manufacturer has embedded any cyber security mechanisms in the ICS, and does not try to determine whether the ICS will integrate with existing cyber security systems or possible future purchases.[44] Alternative ICS products exist, including ones built with "whitelisting" (meaning that they will only respond to specific commands, which is a cyber security measure that could have mitigated or defeated the cyber attack).

1. Claims Against the Chemical Company

As in Scenario One, whether the chemical company had a duty to the victims of the attackers and whether the company violated this duty is likely to be a question of fact. An injured plaintiff might argue that, in light of the company's knowledge of the risks, it was negligent for the company not to investigate the security of the ICS. As in Scenario One, whether that claim will succeed will depend on the foreseeability of the particular attack and other factors.[45]

41. *Id.* at 320.

42. *Id.* at 310-11.

43. Gaines-Tabb v. ICI Explosives, USA, Inc., 160 F.3d 613, 625 (10th Cir. 1998) (rejecting failure-to-warn claims against manufacturers of chemicals used in the Oklahoma City bombing).

44. *See* NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBLICATION 800-82 REVISION 1, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf.

45. *See, e.g.*, Doyle v. Exxon Corp., 592 F.2d 44, 48 (2d Cir. 1979); *see supra* Part I.A.1.a.

2. Claims Against Other Entities

Depending on the nature of the industrial control system used and the nature of the representations the seller made about the system, a plaintiff also might assert that the sellers failed to adequately disclose the limitations of the systems or that defects in the system caused the plaintiff's losses. The plaintiff would need to show that the ICS seller had a duty to the injured plaintiff and that it breached that duty. It is not clear that such a duty would exist.[46]

For the vendor to be liable for an injury, the harm must have been one that the security system was intended to prevent.[47] The liability of the ICS seller may depend on the purpose of the product, and, in particular, whether it was intended to protect against operational problems or intentional attacks.[48]

Whether the company storing the chemicals could assert claims for contribution, indemnity, or breach of contract against the ICS vendor might depend on the terms of the parties' agreement.[49] The company might also assert negligence or products-liability claims against the manufacturer of the control system.[50]

C. Scenario Three

Assume for Scenario Three the same facts as Scenario One, except in this case the cyber security vendor selling products and services to the chemical company makes specific representations regarding the capabilities of its products and services, including that it regularly updates its products and that it is one of the most comprehensive anti-virus products on the market. The company does

46. *See infra* Part I.A; *see also Port Authority*, 189 F.3d at 320 (finding no New York law "which supports the existence of a duty to warn middlemen that consumers, after purchasing their product, may alter the products and harm third parties").

47. *See* Lenox, Inc. v. Triangle Auto Alarm, 738 F. Supp. 262, 267 (N.D. Ill. 1990) (holding that an auto alarm company had a duty to "to install auto alarms in a manner that activates whatever deterrent capacity the alarm may have" but not to "to prevent the theft of plaintiff's jewelry samples" since it was not foreseeable that a plaintiff would store over $100,000 worth of jewelry samples in his car); Collins & Sons Fine Jewelry, Inc. v. Carolina Safety Systems, Inc., 371 S.E.2d 539, 544-45 (S.C. 1988) ("[A] theft by burglary is a reasonably foreseeable consequence of a malfunctioning alarm system.").

48. *See id.*

49. *See* 2 RANDY V. SABETT, 2 INTERNET LAW AND PRACTICE § 27:19 (Westlaw 2013).

50. *See supra* Section I.A.2; *infra* Section I.C.2. *But see* Rustad & Koenig, *supra* note 15, at 1579 ("Although product liability concepts have been extended to durable goods that incorporate software, they have never been applied [to] defective software alone because such causes of action were initially conceived as remedies for personal injury, rather than for financial loss.").

not note, however, that the product does not protect against specifically targeted attacks. Instead, it only says "we regularly update our programs so that you will have best in class protections available." After the attack occurs an audit discovers that the cyber security program would never have stopped the kind of attack that happened. On top of that it is discovered that the cyber security's quality control process was imperfect, such that updates were not sent regularly or timely, and that there was a defect in the software that hackers with moderate to advanced skills could use to deactivate the protections in order to facilitate an attack.

1. Claims Against the Chemical Company

The company would be likely to argue in this scenario that its investigation of the cyber security product and its efforts to mitigate the risk of a cyber attack constituted reasonable care and that it therefore cannot be held liable for negligence. Whether that argument would succeed could depend on the factual question of whether a reasonable entity in the company's position would have undertaken further investigations.

2. Claims Against the Cyber Security Vendor

a. Claims by the Chemical Company

Depending on the terms of the cyber security vendor's agreement with the company, it might be liable to the company for damages arising from the vendor's breach of its agreement.[51] The company might assert contract claims based on the stated scope of services, standard of care, or any warranties or other representations about the product's capabilities, and it might allege that any stated limitations on the vendor's liability did not apply.[52] Whether those claims would succeed would depend on the agreement's language and the particular attack. The vendor might also be liable to the company for negligence if the vendor breached its duty to the company and the parties' agreement did not limit that liability.[53]

51. *See* Mary G. Leary, 72 AM. JUR. 3D *Proof of Facts - Liability for Security or Burglar Alarm System Failure* § 5 (2013).

52. *Cf. id.*

53. *See* Abdallah v. Caribbean Sec. Agency, 557 F.2d 61, 63 (3rd Cir. 1977) ("In those cases dealing with the liability of a burglar alarm company whose system fails to function, it has been held that the company is not liable for the loss on the theory that the burglary was an unforeseeable intervening criminal act breaking the chain of causation. However, while an intervening criminal act usually breaks the chain of causation and thereby negates liability based

The vendor may also be liable to its customer for negligent or intentional misrepresentation, depending on the circumstances.[54] These claims will depend on the whether the inaccuracies in the vendor's statements were "material" to the company's decision to buy the product and the knowledge available to the vendor when it made its statements.[55] In some circumstances, the vendor could be strictly liable for offering a defective product.[56]

b. Claims by Other Parties

As in Scenario Two, the vendor would probably not be liable to non-customers injured in the attack unless a court found that the vendor had a duty to those claimants and its breach of that duty proximately caused their injuries.[57]

A court will probably be reluctant to find that a security system vendor has a duty to claimants other than their own customers, absent unusual circumstances.[58] The seller of a security system is unlikely to

on negligence, where an intervening act is foreseeable, the original actor's negligence may be considered the proximate cause of the loss and he may be liable notwithstanding the intervening criminal act."); 72 AM. JUR. 3D *Proof of Facts - Liability for Security or Burglar Alarm System Failure* § 2 (2013) ("A finding that intervening criminal conduct was foreseeable as a result of the defendant's negligence appears to be particularly likely, or at least may require the submission of the causation issue to the jury, where the original conduct involved was intended to prevent the very harm that occurred, such as where the negligent conduct involved the installation, servicing, or monitoring of a security or burglar alarm system, and a burglary occurs thereafter.").

54. *See* 72 AM. JUR. 3D *Proof of Facts - Liability for Security or Burglar Alarm System Failure* § 4 (2013) (citing case law).

55. *See id.* at §§ 4, 4.5.

56. *See id.* at § 6 ("[U]nder the appropriate circumstances, the negligent manufacturing of a burglar alarm system can be the proximate cause of damages where it is reasonably foreseeable that a defectively manufactured burglar alarm system would increase the likelihood of successful burglaries.").

57. *See* Rustad & Koenig, *supra* note 15, at 1603 ("If terrorists had exploited a security hole in software to conduct illicit communications channels to coordinate [the September 11 attacks], the security hole theoretically could be deemed a cause-in-fact of the billions of dollars of damages that occurred . . . . A court would be unlikely to determine the insecure software a proximate cause of the thousands of deaths and destruction even if the security hole was a cause-in-fact of the attacks.").

58. *See* Cross v. Wells Fargo Alarm Services, 412 N.E.2d 472, 475 (Ill. 1980) (finding that a security service was not liable to a tenant who was injured in a crime); *see also* Gaston Furs Ltd. v. Comet Realty Corp., 640 N.Y.S.2d 485, 486 (N.Y. App. Div. 1996) (finding a security guard service was not liable for building tenant's losses in a theft when the service's "contract with the [building] owner limited its services to the lobby of the building" and "[t]here was no evidence that it assumed a special duty of care to [the tenant]"); New Focus Sportswear, Inc. v. P.J. Fabrico, Inc., 561 N.Y.S.2d 570, 571 (N.Y. App. Div. 1990) (finding that a sprinkler company hired by a building manager did not owe a duty to the customer of a building tenant); SHEPARD'S EDITORIAL STAFF, 6 CAUSES OF ACTION 659, §§ 6.5, 9 (1985) (citing cases).

have a duty to a non-customer when the seller did not accept that obligation and the non-customer did not take action in reliance on the system.[59] In some cases, though, an injured party may be a foreseeable beneficiary of the security vendor's agreement with its customer.[60] If so, the vendor could be liable to injured third parties for breaches of its obligations under the contract.[61]

A duty to third parties may arise if the parties specify that the third parties are intended to be beneficiaries of the agreement or if the vendor's affirmative error "creates or increases an unreasonable risk of harm" or "renders the third-party beneficiary less safe on balance than if no action had been taken at all."[62] An injured party might argue that the defects in the security system created an "unreasonable risk of harm" by failing to protect the company's systems adequately or by negligently misleading the company about the extent of its security protections.[63]

A court might find that vendors of cyber security systems have a duty to at least some non-customers if the parties' agreement specified that a purpose of the controls was to protect third parties or if the vendor's failures unreasonably increased the harm to the non-customers. It is not clear whether that duty would extend to all

59. *See* Gerace v. Holmes Protection of Phila., 516 A.2d 354, 358 (Pa. 1986) (finding that the owner of a ring stolen in a burglary at a jewelry store could not state a claim against the store's security vendor as a third-party beneficiary of the agreement between the store and the vendor), *app. den*. 527 A.2d 541 (Pa. 1987); RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 43 (2012); RESTATEMENT (SECOND) OF TORTS § 324A (1965).

60. *See* Scott & Fetzer Co. v. Montgomery Ward & Co., 493 N.E.2d 1022, 1028 (Ill. 1986) (a fire alarm company had a duty of care to tenants whose premises adjoined its customer's space in a warehouse); RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 43 (2012); RESTATEMENT (SECOND) OF TORTS § 324A (1965) ("One who undertakes . . . to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for physical harm resulting from his failure to exercise reasonable care to protect his undertaking, if (a) his failure to exercise reasonable care increases the risk of such harm, or (b) he has undertaken to perform a duty owed by the other to the third person, or (c) the harm is suffered because of reliance of the other or the third person upon the undertaking.").

61. *See* Phoenix Ins. Co. v. APF Fire Protection, Inc., No. 08 Civ. 7935, 2012 WL 3834743, at *5-6 (S.D.N.Y. Aug. 27, 2012) (finding that a tenant of a building may be considered a third-party beneficiary of a building owner's agreement with a sprinkler maintenance company).

62. *See id.*

63. *Cf.* ADT Security Services, Inc. v. Swenson, 276 F.R.D. 278, 305 (D. Minn. 2011) (denying summary judgment to a security services company on negligence claims when the estate and children of a murdered customer offered evidence that the customer "was lured into a false sense of security by presuming that [the security company] had installed a security system that would provide audible notice when [the murderer] cut the telephone wires and broke into the home").

potential plaintiffs injured by the cyber attack.[64] Even if the cyber security vendor owes a duty of care to parties other than its customers, that duty may be circumscribed by the vendor's agreement with its customers.[65] As a practical matter, that means that third-party claimants may be bound by any contractual limits on negligence liability.[66] Public policy may prevent the vendor from limiting its liability for gross negligence or intentional misconduct.[67]

D. Scenario Four

Company X operates a facility involved in the handling and disposal of extremely hazardous and dangerous materials, such as explosives or highly volatile chemicals. The materials it stores must be kept in a precisely controlled environment, as a change in temperature, humidity, or excessive vibrations could result in catastrophic detonations. Company X has recently automated such controls as a way to exclude the human error element. A cyber security vendor sells Company X hardware and software to prevent the disruption or altering of the key storage controls. Hackers, however, are able to defeat the cyber security controls, causing material changes in storage conditions that lead to explosions with resulting death, injuries, and business interruption for nearby commercial facilities due to the toxic releases and presence of

64. *See* SABETT, *supra* note 49 ("In order for an information security negligence action to prevail, there must initially be a duty between the organization whose system is breached and the third party with which the company has no preexisting contractual arrangement for the company to protect its computer network from threats to its own system . . . . Existing case law is not clear on whether there is such a duty . . . in the case of information security breaches."). However, it may be difficult for third parties to establish the vendor's duty to third parties.

65. *See ADT Security Services, Inc*., 276 F.R.D. at 303 (noting split between courts on the issue and holding that the children of a security system's customer were bound by the limitations on liability in the customer's agreement); John T. Coyne, *Effect of Exculpatory Contractual Provisions on Tort Liability to Third Parties*, 31 TORT & INS. L.J. 785, 785 (1996) ("Courts are divided over whether third-party tort claims are subject to exculpatory contractual provisions that limit the promisor's liability to the promise."); Marjorie A. Shields, Annotation, *Validity, Construction, and Application of Exculpatory and Limitation of Liability Clauses in Burglary, Fire, and Other Home and Business Monitoring Service Contracts*, 36 A.L.R. 6th 305, §§ 21-22 (2008) (citing cases deciding the issue both ways); *but see* Scott & Fetzer Co. v. Montgomery Ward & Co., 493 N.E.2d 1022, 1027-28 (Ill. 1986) (declining to apply contractual limits on liability to claims by third parties).

66. *See ADT Security Services, Inc*., 276 F.R.D. at 303; *cf.* Aphrodite Jewelry, Inc. v. D&W Central Station Alarm Co., Inc., 681 N.Y.S.2d 305, (N.Y. App. Div. 1998) (enforcing exculpatory clauses of contract in a suit by the purchaser of a security system).

67. *See ADT Security Services, Inc*., 276 F.R.D. at 301 (D. Minn. 2011); Cirillo v. Slomin's, Inc., 768 N.Y.S.2d 759, 769 (N.Y. App. Div. 2003) (declining to dismiss a consumer's fraud claims against a security system vendor); Shields, *supra* note 65, §14.

unexploded but live material all around the facility.

1. Claims Against the Chemical Company

As discussed above, a company may have a heightened duty of care when it engages in abnormally dangerous activities.[68] That duty may give rise to strict liability to third parties harmed by the activities.[69]

2. Claims Against Other Entities

The cyber security vendor may be considered to have breached a duty of care to purchasers of its product if a design defect in the control system permitted the cyber attack.[70] Company X may be able to seek common-law indemnification from the cyber security vendor if the company was not itself negligent.[71] Contractual indemnity may also be available, depending on the terms of the parties' agreement.

E. Scenario Five

Assume for Scenario Five the same facts as Scenario Four, except that the cyber security vendor markets its products and services specifically to the companies in the business of handling extremely dangerous materials, like Company X. It markets its products as so robust and well-built that a business like Company X can rest easy knowing that it has bought cyber security products and services designed specifically to protect the incredibly precise requirements of Company X.

1. Claims Against the Chemical Company

In this scenario, the foreseeability of the particular harm that occurred may be greater than in the previous scenarios, since the

68. *See supra* Part I.A.

69. *See supra* Part I.A.2.

70. *See supra* Part I.A.2. *Compare* 72 AM. JUR. 3D *Proof of Facts - Liability for Security or Burglar Alarm System Failure* § 4 (2013) ("Liability under the strict liability doctrine may arise by virtue of a defect in the manufacture of, defect in the design of, or a failure to warn with respect to the use of a security or burglar alarm system."), *with* Aegis Ins. Services, Inc. v. 7 World Trade Co., 865 F. Supp. 2d 370, 384 (S.D.N.Y. 2011) (holding that plaintiff failed to show that a building's alleged design defect caused its damages in a terrorist attack).

71. *See* ERIC C. SURETTE, 41 AM. JUR. *Indemnity* § 21 (2d ed. 2014) ("The exceptions to the rule that indemnity will not be allowed among joint wrongdoers are that a joint wrongdoer may claim indemnity where he or she has not been guilty of any fault, except technically or constructively, or where both parties are at fault, but the fault of the party from whom indemnity is claimed was the efficient cause of the injury.").

company was aware of a specific type of threat.[72] However, as a factual matter, the company may be more likely to have acted reasonably, since it sought to purchase controls to address that specific threat. As in the previous scenarios, the scope of the company's duties and the reasonableness of its precautions are likely to be issues of fact.

2. Claims Against Other Entities

The cyber security vendor may be liable to the company for negligence or even strict product liability in this scenario. A finder of fact is more likely to find that a product was defective when the injury to the plaintiff was the one that the plaintiff sought to guard against when it installed the product.[73] The cyber security vendor may also be liable to Company X for breach of contract or breach of warranty if the vulnerability of the security controls to hackers breached the parties' agreement. Contractual clauses requiring Company X to indemnify or pay contribution to the cyber security vendor for the vendor's liability probably would be enforceable in that situation, although there might be public policy limitations on the scope of that indemnification.[74]

II. APPLICATION OF THE SAFETY ACT TO LIABILITY RESULTING FROM A TERRORIST ATTACK

Given the above scenarios that could result in third party liability claims, the question is what risk-mitigation tools exist that could provide a statutory limit to or eliminate such claims? Based on a review of existing statutes, regulations, and alternative options such as insurance coverage, the best opportunity for limiting liability is the SAFETY Act. "Sellers" of cyber security products or services (a term that also includes companies that develop their own cyber security plans and procedures and then uses them only for internal purposes) are eligible to receive liability protections under the SAFETY Act. Additionally, entities that purchase or deploy SAFETY Act approved cyber security products and/or services will also have the benefit of

72. *See* District of Columbia v. Doe, 524 A.2d 30, 33 (D.C. 1987); RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM §34 (2012) ("When . . . an independent act is also a factual cause of harm, an actor's liability is limited to those harms that result from the risks that made the actor's conduct tortious.").

73. *See supra* Part I.B.

74. *See* SURETTE, *supra* note 71, at § 11 ("Agreements that purport to indemnify another for the other's intentional negligence may be void as a matter of public policy.").

immediate dismissal of third party liability claims arising out of, related to, or resulting from a declared act of terrorism (which encompasses cyber attacks, regardless of whether there is any motive or intent that could be deemed "political" in nature). The basis for this conclusion, as well as the scope of the immediate dismissal offered to customers through the purchase of SAFETY Act approved products or services, is discussed below.

Note that since no litigation specifically involving the SAFETY Act has occurred yet, there is no established legal precedent interpreting the statute itself. However, the fundamental principles of the SAFETY Act are based on the existing common law "government contractor defense," a well-established affirmative defense to third-party litigation. Accordingly, this article is based on interpretations of the SAFETY Act, the Final Rule implementing the SAFETY Act, and the underlying theory of the government contractor defense.

A. Background of the SAFETY Act

The SAFETY Act[75] provides extensive liability protections to entities that are awarded either a "Designation" or a "Certification" as a Qualified Anti-Terrorism Technology ("QATT").[76] Under a "Designation" award, successful SAFETY Act applications are entitled to a variety of liability protections, including:

> All terrorism-related liability claims must be litigated in federal court;
>
> Punitive damages and pre-judgment interest awards are barred;
>
> Compensatory damages are capped at an amount agreed to by both the Department of Homeland Security ("DHS") and the applicant. That damage cap will be equal to a set amount of insurance the applicant must carry, and once that insurance cap is reached no further damages may be awarded in a given year;
>
> A bar on joint and several liability; and
>
> Damages awarded to plaintiffs will be offset by any collateral recoveries they receive (e.g., victims compensation funds, life insurance, etc.)[77]

Should the applicant be awarded a "Certification" under the SAFETY Act for their QATT, all of the liability protections awarded

75. 6 U.S.C. § 441-44 (2013).

76. 6 U.S.C. § 442(a) (2002); 6 C.F.R. § 25.7 (2006).

77. 6 U.S.C. § 442(a); 6 C.F.R. § 25.7.

under a "Designation" are available.[78] In addition, the Seller of a QATT will be entitled to an immediate presumption of dismissal of all third-party liability claims arising out of, or related to, the act of terrorism.[79] The only way this presumption of immunity can be overcome is to demonstrate that the application contained information that was submitted through fraud or willful misconduct.[80] Absent such a showing, the cyber attack-related claims against the defendant will be immediately dismissed.

In order for the SAFETY Act protections to be triggered, the Secretary of Homeland Security must declare that an "act of terrorism" has occurred.[81] The definition of an "act of terrorism" is extremely broad, and includes any act that:

> (i) is unlawful;
>
> (ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
>
> (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.[82]

The Secretary has broad discretion to declare that an event is an "act of terrorism,"[83] and once that has been declared, the SAFETY Act statutory protections will be available to the Seller of the QATT and others. A cursory review of this definition reveals that there is no need to divine a motivation for the attack, and that the language used can (and is) interpreted to include cyber attacks. The only "intent" that must be demonstrated is the intent to cause destruction, injury, or other loss.[84] Accordingly, cyber attacks trigger the protections of the SAFETY Act for cyber security products and tools as well. Moreover, cyber attacks conducted by any entity can be declared an "act of terrorism" under the SAFETY Act regardless of the

78. 6 C.F.R. § 25.8.

79. Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, 71 Fed. Reg. 33,147, 33,150 (June 8, 2006).

80. *Id.* at 33,153-54.

81. 6 U.S.C. § 444(1)-(2) (2013).

82. 6 U.S.C. § 444(2)(b) (2002).

83. *Id.* § 444(2).

84. *Id.* § 444(2)(b)(iii).

motivation or purpose of the group. With that background, we can now explore the protections of the SAFETY Act as extended to purchasers of QATTs.

B. SAFETY Act Protections Available to Customers and Other Entities

One of the most significant additional benefits of the SAFETY Act is that the liability protections awarded to the Seller of the QATT flow down to customers, suppliers, subcontractors, vendors, and others who were involved in the development or deployment of the QATT.[85] In other words, when a company buys or otherwise uses a QATT that has been either SAFETY Act "Designated" or "Certified," that customer is entitled to immediate dismissal of claims associated with the use of the approved technology or service and arising out of, related to, or resulting from a declared act of terrorism.

The bases for these expanded protections are clearly set forth both in the SAFETY Act statute and in the Final Rule implementing the SAFETY Act. Both are detailed below.

With respect to the protections offered to entities other than the Seller of the QATT, the SAFETY Act statute states as follows:

> IN GENERAL.—There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. *Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.*[86]

The SAFETY Act statute also reads:

> JURISDICTION.—Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising

85. Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, 71 Fed. Reg. at 33,150 ("Further, it is clear that the Seller is the only appropriate defendant in this exclusive Federal cause of action.").

86. *See* 6 U.S.C. § 442(a)(1) (2002) (emphasis added).

> out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.[87]

The key language in 6 USC Section 442(a)(1) is that the claims arising out of, relating to, or resulting from an act of terrorism "shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers."[88] Further, in Section 442(a)(2), the SAFETY Act states that U.S. district courts shall have original and exclusive jurisdiction for claims that "result or may result in loss to the seller."[89]

The language in 6 U.S.C. Section 442(a)(1) and (a)(2) reads such that terrorism-related claims that have or could have resulted in a loss to the Seller may only be brought in U.S. district courts against the Seller.[90] Nothing in the statute would give rise to claims against other parties who use or otherwise participate in the delivery and use of the QATT.

The Department of Homeland Security (DHS) agrees with this interpretation, and went to great lengths to elaborate upon this point in the preamble to the Final Rule implementing the SAFETY Act statute:

> *Further, it is clear that the Seller is the only appropriate defendant in this exclusive Federal cause of action.* First and foremost, the Act unequivocally states that a "cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology." *Second, if the Seller of the Qualified Anti-Terrorism Technology at issue were not the only defendant, would-be plaintiffs could, in an effort to circumvent the statute, bring claims (arising out of or relating to the performance or non-performance of the Seller's Qualified Anti-Terrorism Technology) against arguably less culpable persons or entities, including but not limited to contractors, subcontractors, suppliers, vendors, and customers of the Seller of the technology.* Because the claims in the cause of action would be predicated on the performance or non-performance of the Seller's Qualified Anti-Terrorism Technology, those persons or entities, in turn, would file

87. *See* 6 U.S.C. § 442(a)(2) (2002).

88. Please note that "non-Federal government customers" refers to commercial entities.

89. 6 U.S.C. § 442(a)(2).

90. See also Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, 71 Fed. Reg. at 33,150.

> a third-party action against the Seller. In such situations, the claims against non-Sellers thus ''may result in loss to the Seller'' under 863(a)(2). *The Department believes Congress did not intend through the Act to increase rather than decrease the amount of litigation arising out of or related to the deployment of Qualified Anti-Terrorism Technology.* Rather, Congress balanced the need to provide recovery to plaintiffs against the need to ensure adequate deployment of anti- terrorism technologies by creating a cause of action that provides a certain level of recovery against Sellers, while at the same time protecting others in the supply chain.[91]

Within the Final Rule itself, the Department also stated:

> There shall exist only one cause of action for loss of property, personal injury, or death for performance or non- performance of the Seller's Qualified Anti-Terrorism Technology in relation to an Act of Terrorism. Such cause of action may be brought only against the Seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyers, the buyers' contractors, or downstream users of the Technology, the Seller's suppliers or contractors, or any other person or entity.[92]

Thus, both the SAFETY Act statute and the Final Rule implementing the law make it clear that when there is litigation involving a SAFETY Act QATT (whether Designated or Certified) alleging that the QATT was the cause, directly or indirectly, of any alleged losses, the only proper defendant in such litigation is the Seller of the QATT. Customers and others are not proper defendants and are entitled to immediate dismissal, because allowing litigation to proceed against customers would be contrary to both the SAFETY Act statute and Congressional intent.

C. Application of SAFETY Act Protections to Cyber Security Vendors and Their Customers

Considering the above, companies that sell or deploy cyber security QATTs, as well as their customers, are entitled to extensive benefits. Sellers of cyber security QATTs are entitled to the broad protections offered under both a "Designation" and a "Certification." Additionally, as discussed in greater detail below, companies that purchase cyber security QATTs are entitled to unmatched liability protections.

---

91. *Id.* (citations omitted) (emphasis added).

92. 6 C.F.R. § 25.7 (2006) (emphasis added).

As explicitly set forth in the SAFETY Act statute and the SAFETY Act Final Rule, the only proper defendant in litigation following an act of terrorism allegedly involving a SAFETY Act Designated and/or Certified QATT is the Seller itself.[93] In this case, the "Seller" would be the cyber security vendor or company that deploys its own internally developed cyber security policies, procedures, or technologies with the QATT being said Certified or Designated cyber security policies, procedures, or even technologies.

The basis for this analysis rests upon the fact that sellers of cyber security QATTs will have received the QATT Designation or Certification, thus conferring upon them specific statutory liability protections. Further, based on the extensive analysis conducted above regarding the applicability of the SAFETY Act statute and Final Rule, buyers of cyber security QATTs will be considered "customers" for SAFETY Act purposes, and therefore entitled to immediate dismissal of claims related to approved cyber security technology or service. Thus, for any of the previously discussed scenarios where liability to third parties could occur, the SAFETY Act can serve as an excellent tool to mitigate or eliminate said liability.

This interpretation is based upon the SAFETY Act statute and Final Rule, both of which make it clear that the purpose of the SAFETY Act is to dramatically limit litigation following a terrorist or cyber attack and narrow the universe of possible defendants as much as possible.[94] In the case of cyber security QATTs, allowing litigation to proceed against customers of those QATTs would be in violation of the plain language of the SAFETY Act. Therefore, claims against the cyber security QATT customers would be an attempt to circumvent litigation against the Seller of the technology, and should not be allowed under the SAFETY Act statute.

Accordingly, customers of cyber security QATTs are entitled to receive significant liability protections as a result of a SAFETY Act Designation and/or Certification to the Seller, and such protections will dramatically limit customers' exposure to potential litigation following a cyber attack. Additionally, the Seller of the cyber security QATT would be entitled to all appropriate protections offered by the SAFETY Act, whether those offered by Designation or the presumption of dismissal offered by Certification. It is important to note that cyber security QATT customers and Sellers could still

93. *See supra* Part II.B.

94. *See supra* Parts II.A-B.

face cyber security related litigation should the Homeland Security Secretary not declare the cyber attack to be an "act of terrorism" or if the claims do not relate to the QATT as defined by the Department of Homeland Security.[95]

CONCLUSION

Entities that are potentially at risk for third-party liability claims following a cyber attack can be materially protected through the SAFETY Act. Users of SAFETY Act-approved cyber security products or services will also receive direct and tangible benefits. The SAFETY Act provides strong liability protections that will flow down to such customers per the language of the SAFETY Act statute and Final Rule. Cyber attacks and cyber security products and services are covered by the language of the SAFETY Act, and thus, such products and services are also eligible to provide dramatically limited litigation and for such litigation to be limited to "Sellers," not "customers."

Certainly not every cyber attack will result in liability for cyber security vendors or their customers, particularly with respect to third party liability. Should such liability occur, however, it can be mitigated or eliminated using the SAFETY Act.

95. With the definition of "act of terrorism" set forth under the SAFETY Act, functionally any unlawful attack intended to cause harm to the U.S., its populace, or its economic interests could be considered a "terrorist" attack. The Secretary has extraordinarily broad discretion with respect to declaring an event an "act of terrorism", and so that should be considered the appropriate boundaries for purposes of the SAFETY Act. No events have been declared acts of terrorism yet, so we still operate in the realm of the hypothetical. It will depend on what party is in office—odds are a Republican administration will consider a broader range of events as "acts of terrorism", and the opposite will hold true for a Democratic administration. However, that is a guess given the absence of any actual declarations by the Secretary of Homeland Security.