University of Michigan Journal of Law Reform

Volume 49 | Issue 4

2016

# What Common Law and Common Sense Teach Us About Corporate Cybersecurity

Stephanie Balitzer
*University of Michigan Law School*

# WHAT COMMON LAW AND COMMON SENSE TEACH US ABOUT CORPORATE CYBERSECURITY

Stephanie Balitzer*

*Network intrusions and the consequential losses of data and confidentiality plague corporations. With each of these breaches, corporations suffer financial and reputational losses, leaving them scrambling to defend their networks and curb future hacks. Moreover, because their attackers strike from around the globe, are fueled by many motivations, and have ample tools at their disposal, hacks can be almost impossible to predict. The imperfect legal framework in this area only exacerbates this climate of uncertainty. Although active defense strategies like "hacking back" currently exceed the scope of corporate legal rights, many commentators have advocated for the legalization of these practices in the realm of corporate cybersecurity. This Note argues that active defense strategies do not present a viable option for corporations, as they contravene well-developed common law property principles and would generate several negative legal and practical consequences. Instead of deregulating the sphere of corporate cybersecurity to permit corporations to hack back, the Cyber Threat Intelligence Integration Center (CTIIC) should utilize its expertise and functionality as an inter-agency data repository to formulate regulations in conjunction with the Federal Communications Commission (FCC). Such regulations, which would clarify the scope of permissible corporate cyberdefense strategies, would create a viable and sustainable framework for corporations to follow.*

## INTRODUCTION

Cybersecurity has emerged as one of the most challenging problems of the modern era. Corporations face immense obstacles navigating technical and legal frameworks to ensure the confidentiality and integrity of their data and their consumers' personal information.[1] Unfortunately, this corporate cybersecurity problem is growing. In response, many commentators argue that the law should authorize corporations to engage in active defense and, more specifically, hacking back. This solution is not tenable, however, because it effectively sanctions vigilantism and presents the

* J.D. Candidate, University of Michigan Law School, 2016; B.A., Tufts University, 2010. I would like to thank my fellow editors of the Michigan Journal of Law Reform, Professor Julian Mortenson, and my friends Joseph Celentino and Benjamin Reese for their invaluable feedback.

1. *See, e.g.*, Michael Riley, Ben Elgin & Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 17, 2014, 10:31 AM), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

same negative legal and practical consequences as hacking itself. Instead, the newly created Cyber Threat Intelligence Integration Center (CTIIC) should collaborate with the Federal Communications Commission (FCC) to pass regulations that have the capacity to evolve with the changing Internet environment.

This Note examines the challenges of corporate cyberdefense and suggests an approach to mitigate them. Part I outlines the background of the corporate cyberdefense quandary and various cyberdefense strategies. Part II explores the current landscape of cybersecurity law in the United States and the regulatory infrastructure that governs cybercrimes. Part II also surveys case law that illustrates the legal loopholes and ambiguities corporations face when implementing cybersecurity measures. Finally, Part III argues that the proposed active defense model fails to comport with practical concerns and established legal principles. This Note's comparative analysis of common law 'defense of property' principles and corporate cyberdefense provides a framework from which the Federal Communications Commission,[2] in conjunction with the Cyber Threat Intelligence Integration Center, should promulgate sensible and legally-sound corporate cyberdefense guidelines.

## I. A BACKGROUND ON CORPORATE CYBERDEFENSE

The digital era has rendered corporations extremely vulnerable to cyberattacks. The term "cyberattack" is used to describe "deliberate actions" to "alter, disrupt, deceive, degrade, or destroy computer systems or networks" or the information on those networks,[3] or to sabotage or steal corporate assets.[4] As a result of successful cyberattacks, corporations often suffer significant losses.[5] Cyberattacks threaten corporate trade secrets, intellectual property, infrastructure, personally identifiable information (PII), and the integrity of other sensitive information. This Part will detail the

2. The Federal Communications Commission is authorized to regulate "interstate and international communications by . . . wire" and is "the United States' primary authority for communications law, regulation, and technological innovation." FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/general/what-we-do (last visited Apr. 8, 2016).

3. Zach West, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119, 122 (2012) (citing NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009).

4. *See* Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SEDONA CONF. J. 109, 109 (2003).

5. *See Computer Intrusions*, FBI, http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions (last visited Apr. 8, 2016); *see also* West, *supra* note 3, at 128–29.

quantitative and qualitative costs that arise from cyberattacks. It will also offer an example of an intrusion upon a corporate retailer's network that demonstrates the severity of such costs. It will conclude by illustrating how breaches occur and the possible actions corporations may take to defend against such breaches.

### *A. An Examination of the Costs of the Breach Problem*

#### 1. Quantitative Costs

Breaches of corporate networks create significant quantitative losses. According to an IBM study, each data breach costs a compromised company an average of $6.5 million dollars, or $217 for each lost or stolen record.[6] Forty-nine percent of those breaches occurred as a result of a malicious attack.[7] Hacking also affects consumers: according to an IC3 report,[8] the FBI received 262,813 consumer complaints in 2013, in which consumers reported a total of $781,841,611 in losses.[9]

Trends in cybercrime indicate that rates of attack will continue to increase, and that these attacks will grow more sophisticated.[10] Hackers have recently employed newer schemes, including spear phishing,[11] emails containing embedded hyperlinks, "watering-hole attacks,"[12] and other sophisticated tactics. Moreover, according to the Vice President of Dell's Public Sector Software division, "'malware is going to become the tool of choice . . . because it's easy to build" and "the level of sophistication for malware is going

---

6. Ponemon Institute, *2015 Cost of Data Breach Study: United States*, IBM, 1 (May 2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.pdf.

7. *Id.* at 2.

8. *See* FBI, *FBI Internet Crime Complaint Center 2013 Report*, INTERNET CRIME COMPLAINT CENTER, (Nov. 9, 2014 8:51 PM), https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf.

9. *Id.* at 3.

10. *See* Symantec Internet Security Threat Report, SYMANTEC, at 5; WARREN L. DAVIS IV & DANIEL M. DUNLAVY, HYBRID METHODS FOR CYBERSECURITY ANALYSIS LDRD FINAL REPORT 7 (2014).

11. Spear phishing is "an email that appears to be from an individual or business that you know" but is actually from hackers seeking "credit card and bank account numbers, passwords, and . . . financial information." *Spear Phishing: Scam, Not Sport*, NORTON BY SYMANTEC, http://us.norton.com/spear-phishing-scam-not-sport/article (last visited Apr. 8, 2016).

12. A watering-hole attack is "a targeted attack designed to compromise users within a specific industry or function by infecting a website they typically visit and luring them to a malicious site." *Threat #6 Watering Hole*, PROOFPOINT THREATINSIGHT, (Nov. 9, 2014 10:43 PM), https://www.proofpoint.com/us/threat-insight/introduction-to-threats.

to become higher and higher.'"[13] These trends indicate that, not only are hacking costs not going anywhere, but they are likely on track to increase.

### 2. Qualitative Costs

Damage from data breaches extends beyond the quantitative and also includes qualitative losses. Data breaches frequently cause a public relations 'nightmare,' as both investor and consumer confidences in the corporation typically plummet following a breach.[14] Cyberattacks may also significantly undermine a company's competitive advantage—reflected by a host of losses, including trade secrets, drop of stock prices, and loss of jobs.[15]

### 3. Case Study: The Target Breach

The December 2013 Target data breach illustrates the severe costs that arise from hacks. In that attack, sophisticated hackers installed malicious software on Target's network, allowing them to steal forty million credit and debit card numbers, in addition to email addresses, login credentials, and other PII.[16] In total, the breach compromised the PII of about seventy million customers.[17]

Unsurprisingly, this breach shook the corporation. Executive employees, including the CEO and CIO, lost their jobs.[18] Members of the board came under fire.[19] Law enforcement and other government entities, including the Department of Justice, Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC) investigated the incident.[20] The breach also caused a wave of

13. Aaron Boyd, *Malware Getting More Advanced, Easier to Use in 2015*, FEDERAL TIMES (Jan. 19, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/01/19/malware-attacks-advanced-2015/21108035/.

14. *See* Symantec Internet Security Threat Report, *supra* note 10, at 13.

15. *See* Sam Young, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659, 661 (2013).

16. Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, WALL STREET J., (Jan. 10, 2014, 8:36 PM), http://online.wsj.com/articles/SB10001424052702303754404579312232546392464.

17. *Id.*; *see also* Teri Radichel, *Case Study: Critical Controls that Could Have Prevented Target Breach*, SANS INST. 1, 2 (Aug. 5, 2014), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

18. *Id.* at 4.

19. *Id.*

20. *Id.*

disruption to other industries, including the banking sector.[21] Banks were not only required to reimburse customers for their losses, but also had to issue new credit cards to those affected by the breach, costing hundreds of millions of dollars.[22] Banks responded by suing Target.[23]

Consumers also felt the enormous impact as the number of identity thefts multiplied.[24] Months after the breach, studies revealed decreases in consumer perception of Target's customer service, pricing, product selection, quality, and general reputation.[25] Target's earnings plummeted; fourth quarter 2013 earnings dropped forty-six percent.[26] Target's breach provides a valuable lesson in the serious qualitative and quantitative losses that network breaches can inflict.

### *B. How Do Breaches Happen?*

Both state and non-state actors perpetrate cyberattacks.[27] Hackers may be domestic or international and may act as individuals, as part of a broader organization, or as "insiders."[28] Malicious insiders, typically disgruntled employees, seek to exact revenge or to profit from white-collar criminal activities such as identity theft.[29] Criminal organizations also play a role in a substantial portion of data breaches; a Symantec report noted that "[m]ore than [ninety] percent of records breached in 2008 involved groups identified by law enforcement as organized crime."[30] In addition, some hackers belong to collectives such as Anonymous or LulzSec, entities primarily known for engaging in "hacktivism."[31] State actors also perpetrate a

21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.*
25. Adriana Cheng, *Target Data Breach Has Lingering Effect on Customer Service, Reputation Scores*, WALL STREET J. (Apr. 2, 2014, 12:40 PM), http://blogs.marketwatch.com/behindthestorefront/2014/04/02/target-data-breach-has-lingering-effect-on-customer-service-reputation-scores/.
26. SANS INST., *supra* note 17, at 4.
27. *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities Before the Subcomm. on Cybersecurity, Infrastructure Prot., & Sec. Tech. of the House Comm. on Homeland Sec'y*, 113th Cong. 8 (2013).
28. *Id.*
29. Symantec, *Anatomy of a Data Breach: Why Breaches Happen and What to Do About It*, SYMANTEC, 5 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf.
30. *Id.* at 3.
31. Swathi Padmanabhan, *Hacking for Lulz: Employing Expert Hackers to Combat Cyber Terrorism*, 15 VAND. J. ENT. & TECH. L. 191, 193–94, 199–204 (2012).

large number of attacks on American corporations,[32] and many commentators have pointed to China's role in particular.[33] Attacks attributable to China alone purportedly account for one trillion dollars in intellectual property theft per year.[34]

Hackers' motives are as varied as the perpetrators themselves. Some are motivated by profit.[35] Individuals and organized criminal enterprises may seek to sell stolen data (e.g., credit card numbers, PII, or intellectual property) on the black market.[36] Further, some hackers may seek to steal intellectual property or trade secrets to enhance their competitive advantage,[37] while others are motivated by "bragging rights" or glory in the hacker community.[38] Groups such as Anonymous hack in an attempt to "make political statements, cause laughter, and expose holes in the security protocols of both governments and businesses."[39] Finally, state actors or terrorists may vie to obtain confidential intelligence, a goal with potential national security implications.[40]

### *C. Existing Defense Strategies*

Cyberdefense strategies fall into two main categories: active and passive defense.[41] Passive defense strategies generally encompass those strategies that block intruders from entering a network, whereas active defense strategies involve corporations proactively engaging hackers. The sections that follow examine these strategies and how corporations may employ them.

---

32. *See* West, *supra* note 3, at 123–24.

33. *See id.*

34. *Id.*

35. *See id.*

36. LILLIAN ABLON, MARTIN C. LIBICKI & ANDREA A. GOLAY, MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR 4, 8–9 (2014); *see also* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 12, *1 (2014) (noting that banks are the most commonly targeted organizations).

37. *See Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities Before the Subcomm. on Cybersecurity, Infrastructure Prot., & Sec. Tech. of the House Comm. on Homeland Sec'y*, 113th Cong. 8, 7 (2013).

38. *Id.*

39. Padmanabhan, *supra* note 31, at 198.

40. *Id.* at 194.

41. Jan E. Messerschmidt, Note, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUMB. J. TRANSNAT'L L. 275, 290–91 (2013).

### 1. Passive Defense

Corporations use several passive defense strategies that employ perimeters and sensors to block hackers and alert systems security personnel of potential breaches.[42] Those strategies typically fall into one of four categories: "system access controls, data access controls, security administration, and secure system design."[43]

First, system access controls include several intuitive, but critical, security practices which provide for identification and authentication.[44] System access controls "prevent unauthorized users from getting into a system, and force authorized users to be security conscious."[45] For example, a system will deny access to undefined users.[46] Password standards also furnish access control. Standards include the required modification of default passwords, minimum password length and complexity, and the periodic change of passwords for all user accounts.[47] A system might also require users to employ devices such as tokens or biometric data such as fingerprints or retina scans to log in.[48]

Second, data access controls require authorization.[49] Accordingly, users cannot access files without the proper assignment of rights. Unlike system access controls, data access controls restrict network users' abilities to read or edit particular files on the system.[50]

---

42. *See* Teplinsky, *infra* note 139, at 314; Lieutenant Commander Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 2010 MIL. L. REV. 1, 3 n.5 (2009).

43. *Id.* at 21.

44. *Id.* at 22.

45. *Id.*

46. Access control systems employ authentication processes to deny some users because they are "undefined," or because they do not have any designated label in the system. *Legacy Authentication*, CHECK POINT SOFTWARE TECHNOLOGIES, https://sc1.checkpoint.com/documents/R76/CP_R76_SGW_WebAdmin/6721.htm (last visited Apr. 8, 2016); *Fundamentals of Information Systems Security: Access Control Practices*, WIKIBOOKS, http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Practices (last visited Apr. 8, 2016).

47. *Fundamentals of Information Systems Security: Access Control Practices*, WIKIBOOKS, http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Practices (last visited Apr. 8, 2016).

48. Sklerov, *supra* note 42, at 22. According to Sklerov, tokens "contain electronic code that allows access [to] a system, and may even be so sophisticated as to continually calculate new passwords based on time of day or secure algorithms. The computer system being accessed will have matching information to the security device, and will grant access once the petitioning party's password matches." *Id.* at 22 n.130.

49. *Id.* at 23.

50. *See, e.g, Thomson Reuters Data Access Control System (DACS), (DACS, Open DACS Permissions Server, DACS On-Demand): Administering Your Enterprise Information Flows,* THOMSON

The third type of passive defense, security administration, represents "the human side of computer security."[51] Security administration techniques require that an organization educate personnel on best practices, as well as write and enforce security policy.[52] Further, security administration involves "penetration testing" and preparing and planning for disasters.[53] Security administration plays a critical role in thwarting malware and social engineering attacks, which rely upon employees to unwittingly give hackers system access.[54]

Fourth and lastly, corporations employ secure system design, which defends networks with both hardware and software.[55] For example, network segmentation and gateways[56] along the network constitute important system design features that separate portions of the network that contain sensitive information.[57] Further examples include anti-virus programs,[58] encryption programs,[59] firewalls,[60] and intrusion detection systems.[61]

---

REUTERS (2012), http://thomsonreuters.com/content/dam/openweb/documents/pdf/tr-com-financial/dacs.pdf.

51. Sklerov, *supra* note 42, at 23.

52. *Id.* at 23–24.

53. *Id.* Penetration testing is defined as "the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access . . . . [T]he goal of a penetration test is to increase the security of the computing resources being tested." *Penetration Testing: Assessing Your Overall Security Before Attackers Do*, SANS INST. 3 (June 2006), http://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635.

54. Boyd, *supra* note 13.

55. Sklerov, *supra* note 42, at 24.

56. A gateway is "implemented at the boundary of a network to manage all the data communication that is routed internally or externally from that network." *Gateway*, TECHOPEDIA, http://www.techopedia.com/definition/5358/gateway (last visited Apr. 8, 2016).

57. *See* Sklerov, *supra* note 42, at 24 nn.151–52; *Network Segmentation*, SECURE STATE, http://www.securestate.com/Services/Risk%20Management/Pages/Network-Segmentation.aspx (last visited Apr. 8, 2016).

58. Anti-virus software "keeps hackers out by checking against a malicious code spotted on computers . . . [b]ut hackers increasingly use novel bugs," so antivirus software "catches just 45% of cyberattacks." Danny Yadron, *Declaring Antivirus Software Dead, Firm Turns to Minimizing Damage from Breaches*, WALL STREET J. (May 4, 2014 10:41 PM), http://www.wsj.com/articles/SB10001424052702303417104579542140235850578.

59. Encryption programs encrypt files on the system in a plethora of different ways, depending on the manufacturer of the encryption system. Sharon D. Nelson & John W. Simek, *Law Office Security: Building the Castle Moat*, VT. B.J. 25, 29, 31 (2002).

60. Firewalls are "software or software/hardware installations that investigate the network traffic and make a decision to allow it through or block it . . . [t]ypically, firewalls are placed at the first external network entry point, thereby protecting all internal resources." *Id.* at 27–28.

61. *Id.*

### 2. Active Defense

Parties engage in active defense when they use electronic force to counterattack[62] before, during, or in retaliation to a cyberattack.[63] Active defense proponents classify these strategies into three categories: detection and forensics, deception, and attack termination.[64]

Detection and forensics involves threat assessment or attack attribution to identify potential or successful attackers.[65] This investigative work can include both local and remote intelligence gathering.[66] In local intelligence gathering, corporate security professionals may look to a company's network traffic data and malware.[67] Honeypots—"decoy servers or systems set up to gather information regarding an attacker or intruder"—provide another example of a local intelligence gathering method.[68] Security professionals deploy honeypots to attract hackers and identify them based on patterns of practice unique to an individual hacker.[69] Honeypots contain different types of documents, and accordingly provide the opportunity to observe which files intruders attempt to take from the network.[70] Honeypots may therefore help security professionals attribute attacks to particular hackers and better understand their motives.[71]

Corporations may also reach outside of their networks to gather information and evidence on attackers.[72] In such cases, corporate cyber professionals intrude upon an attacker's server and "take any number of actions, including scanning the computer, loading software on it, removing data, encrypting data, deleting data, and stopping the computer from functioning."[73] Security professionals may also use a hacker's own computer camera to photograph the

62. Sklerov, *supra* note 42, at 21–22.

63. Irving Lachow, *Active Cyber Defense: A Framework for Policymakers*, CTR. FOR NEW AM. SECURITY 1 (Feb. 2013), http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

64. *See, e.g.*, *id.* at 5–6.

65. *Id.* at 5.

66. Jody Westby, *Caution: Active Response to Attacks Has High Risk*, FORBES (Nov. 29, 2012 10:52 AM), http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

67. *Id.*

68. *Intrusion Detection FAQ: What is a Honeypot*, SANS INST., https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9 (last visited Apr. 8, 2016).

69. Lachow, *supra* note 63, at 5.

70. *Id.*, at 6.

71. *Id.*

72. *Id.*

73. *Id.*

hacker.[74] Another active defense strategy, "beaconing," occurs when stolen files provide their own location.[75] Those documents may ultimately self-destruct as well.[76] Under such a security model, corporations could also execute a "denial of service attack" or dispatch a virus against the hacker.[77] Notably, "[r]emotely gathering intelligence or actively tracing an attacker without the parties' cooperation or knowledge requires breaking into systems to review logs and seek[ing] traces of the malware or evidence of the network attacks."[78]

Cybersecurity professionals may also practice deception as an active defense strategy. For example, a company might plant files on its system that contain inaccurate information.[79] This false information adjusts the cost-benefit analysis that hackers conduct, as it alters the potential value of the information obtained from a potential hack.[80]

Lastly, a corporation can use attack termination strategies. Examples of attack termination strategies include severing the connection between an infected corporate computer and the attacker's server, and installing patches on other infected computers outside of the network.[81]

## II. CURRENT STATE OF THE LAW

### *A. What Laws Currently Govern Cybersecurity?*

The legal boundaries for network security have evolved significantly over the past few decades. Since 1986, Congress has expanded the scope of criminal sanctions pertaining to data theft and intrusions. This Part describes some of the most important federal legislation governing this field. It then notes various cases in this area that demonstrate loopholes and oversights in the law. Although effective in some respects, these laws leave gaps in enforcement that render corporations vulnerable to attack and fail

74. Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 1, 4 (2014).

75. *Id.* at 11. Harrington discusses the ambiguities surrounding the potential legality or illegality of beaconing. *Id.* at 9–10.

76. *Id.* at 9.

77. These attacks would functionally cause the hacker's computer to stop working. Shane McGee, Randy V. Sabett & Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 12 (2013).

78. Westby, *supra* note 66.

79. Lachow, *supra* note 63, at 6.

80. *Id.*

81. *Id.* at 6–7.

to provide adequate notice of which defense strategies remain legally permissible.[82]

### 1. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030

Congress passed the Computer Fraud and Abuse Act (CFAA) in 1986 to "protect[ ] computers in which there is a federal interest—federal computers, bank computers, and computers used in or affecting interstate and foreign commerce. The Act shields the computers from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud."[83] More specifically, the CFAA criminalizes (1) "obtaining national security information," (2) "accessing a computer and obtaining information," (3) "trespassing in a government computer," (4) "accessing a computer to defraud and obtain value," (5) "intentionally damaging by knowing transmission," (6) "recklessly damaging by intentional access," (7) "negligently causing damage and loss by intentional access," (8) "trafficking in passwords," and (9) "extortion involving computers."[84]

According to a Department of Justice report, lawmakers intended this statute to protect against computer crimes while maintaining the integrity of the federalist system.[85] Legislators thus left space in this statute for the states to address computer crimes by constraining federal jurisdiction to cases creating a compelling federal interest.[86] Since the Act's enactment in 1986, Congress has amended the CFAA eight times, most recently in 2008.[87] One of these amendments added a civil cause of action.[88]

Violations of the CFAA can result in a misdemeanor or a felony charge.[89] If the information obtained is worth less than $5,000, the

---

82. *See* Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1233 (2014) (noting that "current law is ambiguous regarding private sector counterattacks").

83. CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 1 (2014).

84. *See* OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, PROSECUTING COMPUTER CRIMES 3 (2010) (internal formatting omitted).

85. *Id.* at 1.

86. *Id.* at 1–2.

87. *Id.* at 2.

88. 18 U.S.C. § 1030(g) (2008); *see also* Deborah F. Buckham, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. §1830)*, 174 AM. L. REP. FED. 101 (2001).

89. OFFICE OF LEGAL EDUC., *supra* note 84, at 20.

perpetrator may be charged with a misdemeanor.[90] However, if the information is worth more than $5,000, if "commercial advantage or private financial gain" motivated the crime, or if the perpetrator committed the intrusion in furtherance of a separate violation, then the government may charge a felony.[91]

### 2. Wiretap Act, 18 U.S.C. § 2511

The federal government can also prosecute corporate networks intrusions under the Wiretap Act.[92] This statute applies to any person who attempts or successfully intercepts "any wire, oral, or electronic communication."[93] Under this statute, computer network transmissions are considered a type of electronic communication.[94]

This statute provides for the prosecution of any person who "intentionally discloses, endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication."[95] Similarly, this statute prohibits the intentional use of the illegally obtained contents of an electronic communication.[96]

A prosecutor may charge a perpetrator of a Wiretap Act violation with a felony that carries a maximum prison sentence of five years and a monetary fine of $250,000 for individual violators and $500,000 for organizations.[97]

### 3. Stored Communications Act (Electronic Communications Privacy Act), 18 U.S.C. § 2701

The Stored Communications Act addresses the security of stored Internet communications, such as emails.[98] In addition to the protection of communications, this Act guards users who outsource

90. 18 U.S.C. § 1030 (2008).
91. *Id.*
92. *See* OFFICE OF LEGAL EDUC., *supra* note 84, at 59.
93. *Id.* at 60.
94. *Id.* at 59.
95. *Id.* at 73.
96. *Id.* at 77.
97. *Id.* at 87.
98. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208–11 (2004).

data storage.[99] According to the Executive Office for U.S. Attorneys, "[a]t heart, section 2701 protects the confidentiality, integrity, and availability of these communications stored by providers of electronic communication services pending the ultimate delivery to their intended recipients."[100] This Act allows the federal government to charge unauthorized or excessive, intentional access to a "facility through which an electronic communication service is provided" and which "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[101] Individuals committing these acts for commercial gain or advantage face felony charges.[102]

### 4. Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028

Under the Identity Theft and Assumption Deterrence Act, a person may not "knowingly transfe[r], posse[ss], or us[e], without lawful authority, a means of identification of another person with the intent to commit or to aid and abet . . . any unlawful activity."[103] Given that many hacking incidents involve the theft of personal information,[104] the government can use this statute to prosecute such crimes.[105]

A violation of 18 U.S.C. § 1028 can result in imprisonment for up to fifteen years in addition to fines—for example, where the value of the stolen information is of a value of $1,000 or more.[106] Information that comprises a value of under $1,000 carries a maximum of a five-year term of imprisonment.[107]

---

99. *Id.* at 1213–14.
100. OFFICE OF LEGAL EDUC., *supra* note 84, at 89.
101. 18 U.S.C. § 2701 (2002).
102. OFFICE OF LEGAL EDUC., *supra* note 84, at 89.
103. 18 U.S.C. § 1028 (2006).
104. Personal information often includes social security numbers, dates of birth, driver's licenses, or biometric data. OFFICE OF LEGAL EDUC., *supra* note 84, at 97.
105. *Id.* at 96.
106. 28 U.S.C. § 1028(b) (2006).
107. *Id.*

### 5. Access Device Fraud Statute, 18 U.S.C. § 1029

The Access Device Fraud Statute imposes criminal penalties for those engaging in activities such as phishing.[108] More specifically, the statute prohibits a person who knowingly and intentionally "defraud[s], produces, uses, or traffics in one or more counterfeit access devices."[109] The Access Device Fraud Statute (ADFS) defines access devices as "any card, plate, code, account number, electronic serial number . . . personal identification number," or "other means of account access" that can be used to acquire "money, goods, services, or any other thing of value."[110] Hence, this statute applies to intrusions that subsequently result in the sale of any bank account or credit card.[111] Prosecutions under the Access Device Fraud Statute can result in maximum of a ten or fifteen year prison term, depending on the precise section of the statute violated.[112]

### 6. Other Statutes

In addition to the above-described statutes, the government uses several other statutes to address network intrusions. First, under the Wire Fraud statute (18 U.S.C. § 1343), the government can punish Internet-based fraud as a stand-alone crime and as a predicate RICO charge.[113] Next, the government can pursue charges against hackers under the Communication Interference Act (18 U.S.C. § 1362).[114] This statute prohibits the willful or malicious destruction of any means of communication "operated or controlled by the United States."[115] Because of the broad language of this statute, this charge would likely apply to many corporate communication lines as well.[116] Finally, in October 2015, the Senate passed the Cybersecurity Information Sharing Act (CISA).[117] (This bill still faced

108. OFFICE OF LEGAL EDUC., *supra* note 84, at 102–03.

109. 18 U.S.C. § 1029 (2012).

110. *Id.*

111. OFFICE OF LEGAL EDUC., *supra* note 84, at 97.

112. *Id.* at 103.

113. *Id.* at 109–10.

114. *Id.* at 110–11.

115. *Id.* at 111.

116. *Id.*

117. Aarti Shahani, *Senate Approves Cybersecurity Bill: What You Need to Know*, NPR (Oct. 27, 2015 6:06 PM), http://www.npr.org/sections/alltechconsidered/2015 /10/27/452338925/senate-approves-cybersecurity-bill-what-you-need-to-know.

vetogates, including the House of Representatives, as well as a potential veto by President Obama at the time this Note was published.)[118] CISA aims to promote voluntary, but not mandatory, corporate cyber threat information sharing.[119] Moreover, it eliminates any legal liability for corporations who hand over private consumer data to the government.[120]

### *B. What Loopholes Persist in Spite of Legislation?*

As the above-described statutes demonstrate, Congress legislated on a number of cybersecurity issues. In spite of these efforts, statutes often target narrow problems and do not adequately protect specific corporate cybersecurity needs or clarify their defensive boundaries.[121] These failures arise for two primary reasons. First, defendant hackers can exploit technical difficulties between their activity and that specified under the statutory scheme. Second, Congress oftentimes did not intend for these statutes to target the activity at issue.

In *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore LLC*, the Third Circuit held that plaintiffs could not prove their claim that a former employee and consultant violated the Computer Fraud and Abuse Act.[122] The court reasoned that the plaintiffs could not prove that defendants intruded upon the network "knowingly and with intent to defraud," and "as a result . . . furthered the intended fraudulent conduct and obtained anything of value."[123] The court stated that, without proof of the alleged taking or use of information by the defendants, who subsequently started a rival business, the plaintiffs could not meet their burden.[124]

A year earlier, in *United States v. Larry Lee Ropp*, a federal district court granted defendant's motion to dismiss an indictment for

---

118. *See* Andy Greenberg & Yael Grauer, *CISA Security Bill Passes Senate With Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015 5:30 PM), http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.

119. *Id.*

120. *Id.*

121. To date, the Cybersecurity Information Sharing Act, which has not yet been enacted as law, is the most relevant cybersecurity statute passed by Congress.

122. 428 F.3d 504, 506, 513 (3d Cir. 2005).

123. *Id.* at 509.

124. *Id.*

Wiretap Act violations.[125] The government alleged that the defendant installed a keylogger on the victim's desktop.[126] The court concluded, however, that the defendant did not violate the Wiretap Act because "the transmission of keystrokes from a keyboard to a computer's processing unit is not the transmission of an electronic signal by a system that affects interstate commerce," and therefore did not qualify as an electronic communication.[127]

Finally, in *Hilderman v. Enea TekSci, Inc.*, a district court narrowly defined the scope of the Stored Communications Act.[128] The court held that a laptop did not qualify as a "facility through which an electronic communication service is provided," and therefore reading email messages stored on the laptop could not constitute a violation of the Stored Communications Act.[129] The court also determined that emails did not suffice as "electronic storage," because they were not "in temporary, intermediate storage."[130]

Congress did not design the statutes employed in the aforementioned cases to target the specific problem of corporate cybersecurity, but rather to address other niche security problems. The Identity Theft and Deterrence Act, as well as the Access Device Fraud Statute, exemplify the ill-fit between the legislative intent underlying current statutes and corporate cybersecurity.

Although the Identity Theft and Deterrence Act can help the federal government curb hacks, legislative history reveals its limitations.[131] Namely, legislators passed the Act to target the specific problem of identity theft: "a major purpose of this section is to criminalize offenses involving Federal identification documents used 'to support the creation of a new identity.'"[132] In *United States v. Phillips*, for example, the government successfully prosecuted the defendant's enormous hack under this statute only because the stolen data also included social security numbers.[133] There, a university student hacked hundreds of computers at the University of Texas at

125. United States v. Ropp, 347 F. Supp. 2d 831, 832 (C.D. Cal. 2004).

126. "Ropp placed the [keylogger] on the cable that connects [victim's] keyboard to her computer's central processing unit . . . . [T]he [keylogger] recorded and stored the electronic impulses traveling down the cable between her keyboard and the computer to which it was attached. The [keylogger], in this way, 'eavesdrops' on the person typing messages into the computer." *Id.* at 831.

127. *Id.* at 832.

128. Hilderman v. Enea TekSci, Inc., 551 F. Supp. 2d 1183, 1204 (S.D. Cal. 2008).

129. *Id.*

130. *Id.* at 1205.

131. *See* Identity Theft and Assumption Deterrence Act, S. Rep. 105–274, 105th Cong. (2nd Sess. 1998).

132. *Id.*

133. United States v. Phillips, 477 F.3d 215, 218–19, 225 (5th Cir. 2007).

Austin.[134] In the course of these intrusions, the student used scanning tools to steal encrypted data.[135] The Fifth Circuit affirmed the defendant's conviction pursuant to the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028) for "possession of an identification document containing stolen Social Security numbers."[136]

Much like the Identity Theft and Assumption Deterrence Act, the Access Device Fraud Statute (ADFS) serves the narrow purpose of curbing identity theft, and moreover, legislators designed the ADFS specifically to protect financial institutions.[137] In fact, the government agency that enforces the ADFS, the Secret Service, specifically points to the ADFS as a tool to combat the financial industry's significant annual losses from credit card fraud.[138] The narrowly proscribed purpose of the statute makes it of limited use as a tool to combat the diverse nature of cyberattacks.

Although Congress has passed legislation that peripherally addresses issues that relate to corporate cybersecurity, no statutes have passed to date that fully address the unique problems corporations face. Furthermore, none of these statutes address which types of strategies corporations may or may not employ in protecting their networks. Consequently, corporations remain vulnerable to breaches.

### *C. Recent Efforts: Legislative Attempts & Executive Orders*

#### 1. Legislative Attempts

Although cybersecurity has attracted significant political and media attention, Congress has not enacted new legislation in several years. Close to one hundred bills have been introduced to Congress addressing the ever-growing cybersecurity threat to both private industry and government affairs, but privacy concerns,[139] among other problems, have prevented the successful passage of a law. Congress may have taken a step forward, however, with the Senate's recent passage of the Cybersecurity Information Sharing Act.[140]

---

134. *Id.* at 217.

135. *Id.*

136. *Id.* at 218–19, 225.

137. *See Criminal Investigations*, U.S. SECRET SERVICE, http://www.secretservice.gov/investigation/ (last visited Apr. 8, 2016).

138. *See id.*

139. Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 302 (2013).

140. *See* Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015).

### 2. Executive Orders

In reaction to Congressional failures, President Obama issued several executive orders that confront the ongoing problem of cybersecurity.[141] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (2013), provided for the creation of the National Institute of Standards and Technology (NIST) Cyber Security Framework, a voluntary set of standards in best security practices for critical infrastructure.[142] NIST officially issued those standards in February 2014.[143] In October 2014 President Obama authorized Executive Order 13681, aimed to protect consumer financial transactions from identity theft.[144] This order provided parties to federal government transactions with "enhanced security features, including chip-and-PIN technology."[145] In February 2015, President Obama issued Executive Order 13691, which built upon Executive Order 13636.[146] This Order sought to promote information sharing within the private sector and between the private sector and the government.[147] The process advocated under Executive Order 13691 involves cooperation between Information Sharing and Analysis Centers, which are organized by the industry sector, and the Department of Homeland Security.[148]

Additionally, in late February 2015, President Obama created a new national intelligence center—the Cyber Threat Intelligence Integration Center (CTIIC)—under the authority of the Director of National Intelligence.[149] This agency "focus[es] on 'connecting the dots' regarding malicious foreign cyber threats to the nation and

---

141. *See e.g.*, James Arden Barnett Jr., *Cyber Security: Fixing Policy with New Principles and Organization*, in RECENT TRENDS IN NATIONAL SECURITY LAW 25, 25 (Aspatore 2014).

142. *Id.* at 1–2; Exec. Order 13,636, 78 Fed. Reg. 11,739; NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, 3, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (last visited Apr. 8, 2016).

143. *Id.*

144. Exec. Order 13,681, 79 Fed. Reg. 63,491 (2014).

145. *Id.*

146. *See* Exec. Order 13,691, 79 Fed. Reg. 9,349 (2015).

147. *Fact Sheet: Executive Order Promoting Private Sector Cybersecurity Information Sharing*, THE WHITE HOUSE (Feb. 12, 2015), https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform (last visited Apr. 8, 2016).

148. *See Information Sharing and Analysis Organizations*, DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/isao (last visited Apr. 8, 2016).

149. *Fact Sheet: Cyber Threat Intelligence Integration Center*, THE WHITE HOUSE (Feb. 25 2015), https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center (last visited Apr. 20, 2016). Further discussion regarding the CTIIC is included in Part III.

cyber incidents affecting U.S. national interests."[150] The Presidential Memorandum lists the functions of the CTIIC as (1) providing analysis of cyber threats, (2) supporting other government entities in their investigations, (3) overseeing intelligence sharing initiatives, and (4) working to promote information sharing.[151] However, "the CTIIC will not be an operational center" and "will not collect intelligence, manage incident response efforts, direct investigations, or replace other functions currently performed by existing departments, agencies, or government cyber centers."[152]

Finally, in April 2015, President Obama issued Executive Order 13694, which allows the Secretary of the Treasury to authorize sanctions on individuals or entities that use cyber tactics to threaten U.S. national security.[153] The New York Times described this executive order as a measure to treat hackers "the same way [the U.S. government] does terrorists and drug cartels."[154]

Each of these executive orders attempts to address America's massive hacking problem, but none address corporate cyberdefense strategies.

### 3. Remaining Loopholes

Although President Obama's executive orders have made significant strides towards a more coherent and complete approach to corporate cybersecurity, loopholes remain. Corporations lack the requisite protection and guidance regarding boundaries for cybersecurity strategies.

Moreover, the federal government has only passed mandatory cybersecurity requirements for a small sector of private industry.[155]

---

150. *Id.*

151. *Presidential Memorandum – Establishment of the Cyber Threat Intelligence Integration Center*, THE WHITE HOUSE (Feb. 25, 2016), https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat (last visited Apr. 8, 2016).

152. *Fact Sheet: Cyber Threat Intelligence Integration Center*, THE WHITE HOUSE (Feb. 25, 2016), https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center (last visited Apr. 8, 2016).

153. *Fact Sheet: Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, THE WHITE HOUSE (Apr. 1, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/fact-sheet-executive-order-blocking-property-certain-persons-engaging-si (last visited Apr. 8, 2016).

154. Vikas Bajaj, *To Catch a Hacker*, N.Y. TIMES: TAKING NOTE (Apr. 1, 2015, 1:44 PM), http://takingnote.blogs.nytimes.com/2015/04/01/to-catch-a-hacker/?_r=0.

155. *See* Teplinsky, *supra* note 139, at 276.

Although some regulations govern the financial[156] and health[157] spheres, most corporations' network security policies arise from self-regulation.[158] Even NIST's cybersecurity framework is a voluntary set of standards that mostly pertains to critical infrastructure provider networks.[159] One exception is that corporations must now disclose the occurrence of a network breach.[160] While the CTIIC's creation represents a step in the right direction, the center primarily acts to promote information sharing among government agencies and between the public and private sectors.[161] This continued gap in regulatory infrastructure leaves both personal consumer data and corporate assets vulnerable.

Also, the lack of regulatory guidance for corporations makes the legality of several security tools uncertain. Corporations may not fully understand the parameters of permissible active defense strategies,[162] and thereby unwittingly engage in illegal activity without thorough and clear regulations.[163] Additionally, if corporations do not feel adequately protected by the current legal infrastructure, they may be more likely to intentionally resort to illegal strategies.[164] In fact, "[p]rivate companies, including those listed on the

156. For example, in 2001 Congress passed the Gramm-Leach-Billey Act, which compelled security for financial institutions. Those financial institutions were to "implement a comprehensive written information security program to: (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information." Smedinghoff, *supra* note 4, at 110.

157. In 2003 Congress passed HIPAA Security Regulations, which "require covered entities to (1) ensure the confidentiality, integrity, and availability of electronic health information, (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required." *Id.*

158. Teplinsky, *supra* note 139, at 276.

159. *Cybersecurity Framework*, NIST, http://www.nist.gov/cyberframework/ (last visited Apr. 8, 2016).

160. Teplinsky, *supra* note 139, at 277–78.

161. See *Presidential Memorandum – Establishment of the Cyber Threat Intelligence Integration Center*, *supra* note 151; Tom Risen, *New Agency to Aid in Battle Against Hackers*, U.S. NEWS & WORLD REP. (Feb. 10, 2015, 4:25 PM), *available at* http://www.usnews.com/news/articles/2015/02/10/new-cybersecurity-agency-to-aid-in-battle-against-hackers; Dustin Volz, *What a New $35 Million Agency Is Expected to Do for US Cyber Defense*, DEF. ONE (Feb. 10, 2015), http://www.defenseone.com/technology/2015/02/what-new-35-million-agency-expected-do-us-cyber-defense/105048/.

162. *See, e.g.*, West, *supra* note 3, at 130–32 (discussing the contemporary use of active defense strategies and corporate hacking back).

163. *See id.* at 133.

164. *See* Messerschmidt, *supra* note 41, at 277 (describing how Google disclosed that it hacks back); *see also* Huang, *supra* note 82, at 1246, 1251 (noting that "[a]mbiguous legal standards . . . have not stopped security professionals from engaging in some legally questionable tactics," and that "[s]ecurity software vendors sell tools capable of real-time hackback").

Fortune 500, have increasingly turned to self-help measures in response to cyber intrusions."[165] The survey of cases above demonstrates that certain types of hacking activities may be difficult to punish under the current scheme. As previously described, it may be difficult for corporations to prove the actual "harm" or intent element required for criminal prosecution under the current statutory framework.

## III. REFORMS & SOLUTIONS

### *A. Problems with Active Defense*

Active defense strategies will not resolve the gaps corporations face in the current legal climate. These strategies, including hacking back, do not accord with well-developed common law 'defense of property' principles and can create a host of negative externalities. These public policy concerns counsel against allowing corporations to implement many active defense strategies.

#### 1. Application of Common Law Property Law Principles

Common law principles can help identify the most appropriate boundaries for corporate cyberdefense, and case law developed over the course of generations offers a fundamental understanding of how society approaches the defense of property.

Defense of property principles provide a more applicable guide than defense of self. Some commentators[166] argue that, in the cyberdefense context, self defense is the applicable standard under which these questions should be addressed. The crux of this argument is twofold: (1) that the United States government cannot adequately protect corporations because officials would be hesitant to use force against foreign nations; and (2) even assuming that the government would not be hesitant, it would lack adequate resources to defend against cyber threats.[167]

But defense of self principles should not apply in the corporate cyberdefense realm because defense of self presupposes a threat to life or limb.[168] Defense of self requires a sense of immediacy; it assumes that the contemplated action will mitigate or reduce, rather

165. Messerschmidt, *supra* note 41, at 277.
166. *See* McGee et al., *supra* note 77, at 4–5.
167. *See* West, *supra* note 3, at 125–28.
168. *See* 3A GILLESPIE MICH. CRIM. L. & PROC. § 91:51 (2d ed. 2014).

than aggravate, the harm.[169] It does not, however, contemplate action in response to a harm already inflicted,[170] as in a hacking back scenario. Even when corporate cybersecurity professionals detect intrusions while hackers remain in the network, active defense strategies may still be inappropriate. As explained below, common law principles prohibit most forms of force when used in defense of property.

The most legally sound and logical application of these principles can be found in the common law reasonableness requirement for any defense of real and personal property. That requirement limits property owners' available responses to intruders. Still, it may be reasonable for a property owner to confine an individual to prevent or end his intrusion on land or chattels."[171] But the permissibility of this sort of apprehension is limited.[172] For example, in *State v. Schloredt*, the court found that a property owner was not justified in attempting to shoot an intruder on his property.[173] More specifically, the court stated that although a property owner has the right to protect his property, he may not use more force than is necessary.[174] The court, moreover, eloquently described the dangers of such behavior: "'[s]elf-help has always been reckoned as a perilous remedy owing to the stringent rules against its abuse' [ . . . ] a trespass not involving the protection of a home does not justify the use of a deadly weapon or the infliction of great bodily harm."[175]

Without the threat of injury to one's person, use of force may be unreasonable. Consider, for example, *Katko v. Briney*, where the

---

169. Consider, for example, the "retreat to the wall" principle of self defense. In fact, even the right to defend one's own life and limb has caveats, such as the duty to "retreat to the wall." This principle provides that "a man who, in the lawful pursuit of his business is attacked by another, under circumstances which denote an intention to take away his life or do him some enormous bodily harm, may lawfully kill the assailant, provided he uses all the means in his power, otherwise to save his own life or prevent the intended harm; such as retreating as far as he can." 3A GILLESPIE MICH. CRIM. L. & PROC. § 91:51 (2d ed. 2014); *see also, e.g.*, Commonwealth v. Benoit, 892 N.E.2d 314, 326 (Mass. 2008). The "retreat to the wall" principle has been abrogated in thirty-three states, however, under "stand-your-ground-laws." *See* AMERICAN BAR ASSOCIATION: NATIONAL TASK FORCE ON STAND YOUR GROUND LAWS, PRELIMINARY REPORT AND RECOMMENDATIONS 10 (2014). Those laws eliminate the duty to retreat, but still require an objectively reasonable threat or perceived threat to life or limb. *See id.* at 9.

170. *See* 3A GILLESPIE MICH. CRIM. L. & PROC. § 91:51.

171. RESTATEMENT (SECOND) OF TORTS § 80 (1977); s*ee also* Teel v. May Dep't Stores Co., 155 S.W.2d 74 (1941) (finding it reasonable for a department store owner to use reasonable confinement in defense of property).

172. RESTATEMENT (SECOND) OF TORTS §§ 79, 80 (1977).

173. State v. Schloredt, 111 P.2d 128, 131–32 (Wyo. 1941).

174. *Id.* at 131.

175. *Id.*

court held that a "deadly spring gun or other mechanical device" may not be used in defense of property.[176] The defendant attempted to protect an uninhabited home, which had been subject to a host of break-ins and thefts.[177] In response to these threats, the defendant home owner boarded up windows and doors, hung 'no trespass' signs," and created a shotgun trap to injure intruders.[178] When the plaintiff entered the house, the shotgun discharged and the plaintiff intruder was severely injured.[179] The Supreme Court of Iowa ruled that a property possessor may use reasonable force to resist a trespasser, but that here the force was excessive.[180]

Common law principles similarly limit the methods for recapturing property. Recapture is generally permitted when "a person reasonably believes that he has been illegally disposed of real or personal property by another."[181] However, recapture is limited to circumstances of "hot pursuit,"[182] and outside such circumstances, the property owner must seek recourse in court.[183]

Such limitations imposed by common law in defense of property logically apply to the corporate cyberdefense context when only property, rather than life and limb, is in peril. Reasonable force may only be used to *prevent* property loss. Therefore, network security professionals may not use force against intruders after an imminent threat has passed. These principles discredit many active defense strategies. For example, hacking back would not be permissible because it (1) does not respond to an immediate threat; and (2) involves the intrusion upon another network, often with the intent to cause serious harm or to recover data from the hacker's network. Similarly, traps such as hidden malware on corporate networks constitute unreasonable defense of property strategies because they can easily destroy the machine or server onto which they are installed.[184] Moreover, where corporations misattribute a threat, they may unwittingly cause disproportionate

176. WAYNE R. LAFAVE, 2 SUBSTANTIVE CRIMINAL LAW § 10.6 (2d ed. 2015); *see also* RESTATEMENT (SECOND) OF TORTS § 79 (1977) (explaining that use of deadly force for the intrusion of property may only be justified if it is believed that the intruder may cause death or serious bodily injury to the actor or a third party).

177. Katko v. Briney, 183 N.W.2d 657, 658 (Iowa 1979).

178. *Id.*

179. *Id.*

180. *Id.*; *see generally* Hooker v. Miller, 37 Iowa 613 (Iowa 1873); Wilder v. Gardner, 39 Ga. App. 608 (Ga. Ct. App. 1929); State v. Beckham, 257 S.W. 817 (Mo. 1924).

181. WAYNE R. LAFAVE, 2 SUBSTANTIVE CRIMINAL LAW §10.6 (2d ed. 2015).

182. *Id.*

183. *Id.*

184. *See The Offensive Approach to Cyber Security in Government and Private Industry*, INFOSEC INSTITUTE, http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/ (last visited Apr. 8, 2016).

damage or threat to life and limb.[185] If corporations unintentionally hack a server engaged in infrastructural functions, for example those supporting electrical plants, life and limb could be in danger when such plants shut down.[186]

Generally, any active defense strategies that involve remote intrusions would likely be found unreasonable under defense of property common law doctrine. Only two active defense strategies, deception and local intelligence gathering, conform to defense of property principles.

### 2. Public Policy Implications of Hacking Back

Beyond defense of property principles, public policy considerations also counsel against corporate self-help strategies. Those considerations include the following: (1) attribution problems that might incur criminal and civil liability; (2) the better suited skills, experience, and accountability of law-enforcement personnel; (3) the creation of distorted incentives for hackers; and (4) the risk of escalation, particularly in the international sphere.

One concern is that of attribution.[187] Corporations may not have adequate information, technology, procedures, or professionalism to investigate hacking. Instead, they may unintentionally pursue and hack back innocent parties.[188] Attribution is especially difficult in the context of hacking because hackers often use "compromised computers of unwitting third parties."[189] Beyond the social costs of this behavior, corporations may incur liability for such conduct. Private parties or government actors may impose criminal or civil liability against corporations who intrude or cause damage to their networks while seeking retribution.

Our legal system has traditionally taken a dim view of such vigilantism.[190] Law enforcement and the court system are generally better-trained and equipped to deal with investigating and assessing

185. *See* Messerschmidt, *supra* note 41, at 322–23.

186. *See* Bill to Reshape U.S. Cybersecurity, S. 773, 111th Cong. (2009) (explaining the types of dangers posed to critical infrastructure when cyber attacks are executed).

187. McGee et al., *supra* note 77, at 5.

188. Attribution problems could result in corporations attacking white-hat hackers unintentionally. *See* WILLIAM EASTTOM, NETWORK DEFENSE AND COUNTERMEASURES: PRINCIPLES AND PRACTICES (2d ed. 2013).

189. *The Offensive Approach to Cyber Security in Government and Private Industry*, INFOSEC INSTITUTE, http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/ (last visited Apr. 8, 2016).

190. *See* Adam B. Badawi, *Self-Help and the Rules of Engagement*, 29 YALE J. ON REG. 1, 2 (2012).

culpability. Law enforcement officers can be held accountable through official channels and rules.[191] Criminal sanctions, and more specifically, the threat of imprisonment, generally serve as a powerful deterrent to criminal activity.[192] If the government grants corporations the right to hack back, corporations may prefer to engage with hackers on their own, rather than report intrusions to law enforcement. Therefore, hacking back could replace the criminal justice system and remove a powerful disincentive to hack corporations. Moreover, allowing corporate vigilantism would eliminate due process for accused parties.[193] The founding fathers designed our legal system to afford accused parties the benefit of the doubt.[194] Accordingly, self-help strategies contradict the foundational philosophy of our judicial system.

One additional policy concern undermining our legal system's discomfort with self-help mechanisms is the risk of escalation.[195] Corporate hacking back could result in an endless cycle of network intrusions. This runs the risk of abuse—corporations could claim that an intrusion justified a subsequent retributive hack. Moreover, corporate actors might hack foreign state actors. Such behavior undermines U.S. foreign policy, as domestic government actors would no longer have control over what could be considered an act of war.[196] Corporate actors could potentially inspire tensions between the United States and its allies, as well as its enemies.[197] In November 2014, hackers, believed to have operated out of or been supported by the government of North Korea, infiltrated both Sony Entertainment's US and worldwide servers.[198] "The attackers took terabytes of private data, deleted the original copies from Sony

191. *See id.* at n.98.

192. § 2 Definition, Elements of a Crime, Aims of Punishment, CCH INTERNATIONAL ENCYCLOPEDIA OF LAWS CYBER LAW, 2013 WL 4296826.

193. *See* Badawi, *supra* note 190, at 21.

194. Moreover, civil defendants may not be held accountable unless a claim is proven by the preponderance of the evidence, and criminal defendants must be proven guilty beyond a reasonable doubt. *See* In re Winship, 397 U.S. 358, 362–63 (1970).

195. *See* McGee et al., *supra* note 77, at 36.

196. *See generally* Sklerov, *supra* note 42 (analyzing cyberattacks within the framework of the law of war).

197. *The Offensive Approach to Cyber Security in Government and Private Industry*, INFOSEC INSTITUTE, http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/ (last visited Apr. 8, 2016).

198. Timothy B. Lee, *The Sony Hack: How it Happened, Who is Responsible, and What We've Learned*, VOX (Dec. 17, 2014, 9:00 PM), http://www.vox.com/2014/12/14/7387945/sony-hack-explained; Jose Pagliery, *What Caused Sony Hack: What We Know Now*, CNN (Dec. 29, 2014, 1:58 PM), http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/.

computers, and left messages threatening to release the information if Sony did not comply with the attackers' demands."[199] Moreover, hackers shut down Sony's network for several days and posted private information and films online.[200] Although the American government attributed the attack to North Korea, the source of the attack still remains unclear after extensive investigation.[201] Such a case demonstrates the serious risks of permitting corporations to engage in hacking back. If Sony were permitted to hack back North Korean networks, it could result in significant foreign policy discord. The United States already has a contentious relationship with North Korea, and such delicate relationships should not fall into the hands of corporate actors.

These significant costs demonstrate that active defense strategies, including hacking back, will not provide the proper framework for corporate cyberdefense.

### *B. Solutions*

Because of these issues with active defense and hacking back, corporations should instead rely on regulatory guidance regarding permissible cyberdefense strategies. However, the problem is that comprehensive regulatory guidance does not yet exist. The CTIIC should utilize its expertise and functionality as an inter-agency data repository to formulate regulations in conjunction with the FCC—which has Congressionally delegated rulemaking authority—to clarify the scope of permissible corporate cyberdefense strategies. These regulations would have the capacity to evolve with the changing Internet landscape. This is because of the pliancy of regulations relative to statutes. And a FCC regulatory process avoids vetogates, as well as other complications of the political process. Critically, closing legal loopholes will prevent corporations from relying on risky self-help strategies and would require corporate defense strategies to align with well-developed common law principles.

199. Lee, *supra* note 198.

200. *Id.*

201. Lily Hay Newman, *What We Do and Don't Know About the Sony Pictures Hack*, SLATE (Dec. 17, 2014, 4:45 PM), http://www.slate.com/blogs/future_tense/2014/12/17/sony_pictures_hack_what_we_do_and_don_t_know.html.

### 1. Why an Agency is the Proper Vehicle for Reform

An analogy to a previously established administrative agency, the Environmental Protection Agency (EPA), provides a compelling narrative of why this CTIIC-FCC partnership would serve as the proper vehicle for reform.

Throughout the mid-twentieth century, the nation faced enormous environmental troubles—pollutants created a diffuse problem on an enormous scale and involved so many corporations and individuals, that solving the problem must have seemed insurmountable. Then, in December 1970, Congress established the EPA "to consolidate in one agency a variety of federal research, monitoring, standard-setting and enforcement activities to ensure environmental protection."[202] Clear guidance for corporations resulted in enormous successes in environmental cleanup. For example, the EPA has improved water standards and "the number of Americans receiving water that met health standards went from 79 percent, in 1993, to 92 percent in 1998."[203]

The CTIIC-FCC regulations would likely yield similar benefits as those promulgated by the EPA. The data and resources the CTIIC compiles, coupled with FCC regulatory authority and expertise, would provide for such effective regulations.[204] This agency solution would likely result in better social and political outcomes than allowing for corporate vigilantism.

### 2. What the FCC and CTIIC Should Do

The Cyber Threat Intelligence Integration Center should wield its vast data repository and cybersecurity insights to formulate detailed and extensive corporate cyberdefense regulations in conjunction with the FCC.

First, in order to conform to the sound reasoning of common law defense of property principles, corporations should be permitted to continue to use passive defense strategies. Second, the CTIIC should promulgate regulations that explicitly prohibit hacking

---

202. *EPA History*, U.S. ENVTL. PROTECTION AGENCY, https://www.epa.gov/aboutepa/epa-history (last visited Apr. 8, 2016).

203. *40 Years of Achievements, 1970–2010*, U.S. ENVTL. PROTECTION AGENCY, http://www.epa.gov/40th/achieve.html [http://www.epa.gov/40th/achieve.html] (last visited Apr. 16, 2015).

204. *Presidential Memorandum – Establishment of the Cyber Threat Intelligence Integration Center*, *supra* note 151.

back, beaconing, honeypots, and most other active defense strategies. Such regulations might clarify, for example, that while hacking back is impermissible, strategies such as the use of deception and local intelligence gathering remain acceptable. These clarifications will help avoid corporate vigilantism, which holds the potential to stress intricate foreign political relationships and impose enormous externalities on third parties. Additionally, regulations may curb corporate incentives to withhold information from government actors.[205]

Third, these regulations should mandate extensive minimum security standards for corporations based on the CTIIC's extensive study and repository of expertise.[206]

### 3. Potential Criticisms of the Agency Approach

Critics will likely dismiss this proposed regulatory approach on several grounds. Some may criticize the approach as expanding an ever-growing administrative bureaucracy. Other critics may expound upon that negative perception and claim that government actors are not best equipped to deal with such ever-changing, technologically complex, and numerous corporate cybersecurity threats.

Criticism of the overgrowth of the administrative state fails to recognize that agencies such as the EPA have successfully grappled with seemingly insurmountable, complex social and economic ills. If such a move is effective, the expansion of the governmental bureaucracy and budget would seem to be a reasonable trade-off given the escalating costs corporations currently face from hackers. Moreover, such a solution avoids the complications associated with congressional gridlock. The FCC's action here will also allow Congress to avoid political consequences associated with agency rulemaking.

Next, critics may claim that governmental agencies are ill-equipped to handle the magnitude of regulatory and legal enforcement spurred by hacking incidents. They may claim that efficiency

---

205. An Executive Assistant Director of the FBI, Richard McFeely noted that the "biggest issue right now is getting the private sector to a comfort level where they can report anomalies, malware, incidences within their networks. It has been very difficult with a lot of major companies to get them to cooperate fully." Michael D. Scott, *18 No. 2 Cyberspace Law 3*, CYBERSPACE LAW. (March 2013).

206. Other commentators have noted the potential effectiveness of mandatory standards. *See* Robert Gyenes, *A Voluntary Cybersecurity Framework is Unworkable – Government Must Crack the Whip*, 14 U. PITTSBURGH J. TECH. L. & POL'Y 293, 310–13 (2014).

would tend to mandate that corporations mitigate their own losses and enforce their own rules. Such a criticism ignores the vast intelligence and criminal enforcement mechanisms that the United States has already mobilized in response to complicated issues such as international terrorism. If agency cooperation, headed by the CTIIC, can encourage cross-agency cooperation in that same way, government can indeed serve as the best enforcement and regulatory mechanism for the corporate cybersecurity quandary.

Overall, like any solution, the CTIIC-supported issuance of regulations by the FCC in this area may not be a perfect one. Given the nature of the issue, however, it appears to be a far superior approach to the hacking back and active defense model solution proposed by others.

## CONCLUSION

Although the magnitude of the corporate cybersecurity problem may seem daunting, resort to common law principles clarify possible solutions and strategies for mitigating the damage inflicted by hackers. Likewise, defense of property principles clarify why some active defense strategies will amplify the costs associated with hacking, rather than alleviate corporate losses. Common law principles show that the FCC, partnered with the CTIIC, should promulgate regulations that clarify the bounds of corporate defensive strategies and aid corporations in securing their digital borders.