Duquesne Law Review

Volume 59 | Number 2 Article 6

2021

The Evolution of Legal Risks Pertaining to Patch Management and Vulnerability Management

James T. Kitchen

David R. Coogan

Keeton H. Christian

The Evolution of Legal Risks Pertaining to Patch Management and Vulnerability Management

James T. Kitchen[*]
David R. Coogan[**] *& Keeton H. Christian*[***]

The views and opinions set forth herein are the personal views or opinions of the author; they do not necessarily reflect views or opinions of the law firm with which [he/she] is associated.

* Partner, Jones Day. Jimmy Kitchen is a former Assistant U.S. Attorney who has led groundbreaking cyber investigations, including one that led to the first-ever corporate cyber-espionage indictment of Chinese military hackers in the landmark case of *U.S. v. Wang Dong*. He assists companies with cybersecurity and breach response and other internal investigations and compliance.

** Associate, Jones Day. David Coogan is a former Marine Corps intelligence officer and prosecutor. He advises companies on cybersecurity and privacy compliance as well as related litigation.

*** Associate, Jones Day. Keeton Christian is a member of the New Lawyers Group.

I. INTRODUCTION

In May 2017, WannaCry malware spread across the globe by exploiting a known vulnerability in Windows called EternalBlue.[1] WannaCry encrypted files on infected Windows systems.[2] The malware impacted schools, hospitals, and businesses in over 150 countries,[3] including the British National Health System, which spent nearly $100 million to fix its systems.[4] Two months earlier, Windows had released patches for the EternalBlue vulnerability.[5] Had the patches been installed, the malware would not have impacted

1. Ionut Arghire, *NSA's EternalBlue Exploit Fully Ported to Metasploit*, SEC. WK. (May 16, 2017), https://www.securityweek.com/nsas-eternalblue-exploit-fully-ported-metasploit.

2. Russell Goldman, *What We Know and Don't Know About the International Cyberattack*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html.

3. *Id.*

4. Danny Palmer, *This Is How Much the WannaCry Ransomware Attack Cost the NHS*, ZDNET (Oct. 12, 2018, 5:59 AM), https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/.

5. *Security Update for Microsoft Windows SMB Server (4013389)*, MICROSOFT, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (Oct. 11, 2017).

the Windows systems.[6] In June 2017, another piece of malware, known as NotPetya, exploited the same Windows vulnerability to cause even more damage.[7] NotPetya irreversibly encrypted computers in a way that made it impossible to recover the computer or the data on it.[8] NotPetya caused large, multinational companies to go offline for weeks and caused billions in damages.[9] It has been called the "most destructive and costly cyber-attack in history."[10]

Not only did the malware impact operations at affected companies, it also had legal impacts. In June 2017, Nuance, a speech recognition software vendor, was a victim of the NotPetya attack, which cost the company more than $90 million.[11] Nuance was also the defendant in two lawsuits brought by two of Nuance's customers.[12] The lawsuits alleged Nuance failed to use reasonable care in its information security practices.[13] Specifically, one of the customers alleged that although in March 2017 the customer had installed the Windows patch for EternalBlue on its Windows systems, Nuance did not.[14] The customer alleged that because Nuance's network had administrator-level credentials to the customer's network, the malware entered the customer's network and caused nearly $11 million in damage.[15]

Each year software and hardware vendors release thousands of updates to patch vulnerabilities in their software.[16] Over the past

---

6. *Customer Guidance for WannaCrypt Attacks*, MICROSOFT SEC. RESPONSE CTR. (May 12, 2017), https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

7. Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 531–32 (2019).

8. *Id.* at 532.

9. Press Briefing, The White House, Statement from the Press Sec'y (Feb. 15, 2018) (archived at https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/).

10. *Id.*

11. Nuance Commc'ns, Inc., Quarterly Report (Form 10-Q) 23 (Feb. 9, 2018).

12. Heritage Valley Health Sys., Inc. v. Nuance Commc'ns, Inc., 479 F. Supp. 3d 175 (W.D. Pa. 2020); Princeton Cmty. Hosp. Ass'n, Inc. v. Nuance Commc'ns, Inc., No. 1:19-00265, 2020 WL 1698363 (S.D. W. Va. Apr. 7, 2020).

13. *Heritage Valley Health Sys., Inc.*, 479 F. Supp. 3d at 188–89; *Princeton Cmty. Hosp. Ass'n, Inc.*, 2020 WL 1698363, at *1.

14. Complaint at ¶¶ 25–26, *Princeton Cmty. Hosp. Ass'n, Inc.*, 2020 WL 1698363 (S.D. W. Va. Apr. 11, 2019) (No. 19-C-59). This lawsuit was jointly dismissed by the parties after the court denied Nuance's motion to dismiss. *See* Joint Stipulation & Order of Dismissal with Prejudice, *Princeton Cmty. Hosp. Ass'n, Inc.*, 2020 WL 1698363 (S.D. W. Va. Aug. 11, 2020) (No. 19-C-59). The other lawsuit was dismissed because the court found that Nuance did not owe a duty to its customer beyond the obligations in the contract between the parties. *Heritage Valley Health Sys., Inc.*, 479 F. Supp. 3d at 187.

15. Complaint, *supra* note 14, at ¶¶ 37, 56.

16. *Is Software More Vulnerable Today?*, EUR. UNION AGENCY FOR CYBERSECURITY (Mar. 12, 2018), https://www.enisa.europa.eu/publications/info-notes/is-software-more-vulnerable-today.

twenty years, the number of vulnerabilities has largely increased each year.[17] Companies that rely on the software and hardware to run their businesses must sift through the deluge of notifications and determine which patch should be prioritized in order to prevent a hacker from exploiting an unpatched vulnerability and using it to get inside the company network.[18] Vendors typically assign a score, using the Common Vulnerability Scoring System (CVSS), to each vulnerability to indicate the likelihood and impact of exploitation.[19] Some vulnerabilities are considered important enough that the United States Department of Homeland Security orders all federal agencies to implement a patch within a particular time period.[20] In fact, in May 2017, President Trump issued an Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure which found that "[k]nown but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies."[21] These "[k]nown vulnerabilities include[d] using operating systems or hardware beyond the vendor's support lifecycle" and "declining to implement a vendor's security patch."[22]

Many data breaches that occur each year are due to unpatched vulnerabilities.[23] Reports vary about how many data breaches are due to known unpatched vulnerabilities. One study reported sixty percent of the breaches could have occurred because a patch was available for a known vulnerability but not applied.[24] Another report found that one in three breaches are caused by unpatched vulnerabilities.[25]

---

17. *National Vulnerability Database: Statistics Results*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/vuln/search/statistics (last visited Mar. 8, 2021). The number of vulnerabilities dramatically increased beginning in 2017. *See* Rob Lemos, *The State of Vulnerability Reports: What the CVE Surge Means*, TECHBEACON, https://techbeacon.com/security/state-vulnerability-reports-what-cve-surge-means (last visited Mar. 8, 2021).

18. *See* Jason Bloomberg, *To Patch or Not to Patch? Surprisingly, That Is the Question*, FORBES (Apr. 16, 2018, 9:10 AM), https://www.forbes.com/sites/jasonbloomberg/2018/04/16/to-patch-or-not-to-patch-surprisingly-that-is-the-question/?sh=4997f33d58fe.

19. *Common Vulnerability Scoring System SIG*, FIRST, https://www.first.org/cvss/ (last visited Mar. 8, 2021).

20. *See, e.g.*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., EMERGENCY DIRECTIVE 20-04, MITIGATE NETLOGON ELEVATION OF PRIVILEGE VULNERABILITY FROM AUGUST 2020 PATCH TUESDAY (2020).

21. Exec. Order No. 13,800, 82 Fed. Reg. 22,391, 22,391 (May 11, 2017).

22. *Id.*

23. Taylor Armerding, *Patch Now or Pay Later: Report*, FORBES (June 6, 2019, 9:37 AM), https://www.forbes.com/sites/taylorarmerding/2019/06/06/report-if-you-dont-patch-you-will-pay/?sh=2e3fe0693acd.

24. PONEMON INST. LLC, COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE 3 (2020).

25. Steve Ranger, *Cybersecurity: One in Three Breaches Are Caused by Unpatched Vulnerabilities*, ZDNET (June 4, 2019, 2:15 PM), https://www.zdnet.com/google-

Although the process of prioritizing and implementing patches is technical and typically not the responsibility of an organization's legal department, unpatched software is a legal risk for organizations. With the evolution of cybersecurity regulation and litigation, legal liability relating to vulnerability and patch management is no longer theoretical.[26] Because software vendors typically notify their customers about vulnerabilities in their software and the availability of updates,[27] regulators may take the position that companies that use the software are generally on notice of the vulnerabilities. Due to the increase in the number of disclosed vulnerabilities and the increased general acceptance of security standards, regulators have been paying greater attention to whether companies are patching known software vulnerabilities. Because company lawyers may not be sufficiently technically knowledgeable to understand the IT department's approach to vulnerability and patch management, it can be a blind spot for the legal department. Conversely, the IT department may not understand the legal implications of the work they do in this arena. This article attempts to bridge that gap.

This article begins with an overview, in non-technical terms, of the tools generally available and processes implemented for vulnerability management and patch management. Section II identifies some of the evolving security standards that regulators and plaintiffs may rely on to show that companies are legally required to have vulnerability management and patch management. Section III identifies U.S. legal implications of vulnerability management and patch management and factors that a court and regulators may consider.

---

amp/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/. The other end of the spectrum is reporting that the root cause of only two percent of breaches was missing patches. *See* SARA BODDY & RAY POMPON, THREAT INTELLIGENCE REPORT: LESSONS LEARNED FROM A DECADE OF DATA BREACHES (2017), https://www.f5.com/content/dam/f5/downloads/F5_Labs_Lessons_Learned_from_a_Decade_of_Data_Breaches_rev.pdf. This report points out that some phishing cases are only successful if the end user's machine is not patched properly. *Id.* at 36 ("For phishing cases that rely on users opening a malicious file (which can then exploit a vulnerability on the system), patch, update, and patch again!").

26. *See generally* STEWART BAKER & MAURY SHENK, A PATCH IN TIME SAVES NINE: LIABILITY RISKS FOR UNPATCHED SOFTWARE, STEPTOE & JOHNSON (Oct. 2003), https://www.steptoe.com/publications/274a.pdf.

27. Cristian Florian, *Security Patching Trends for Major Software Vendors*, TECHTALK (Mar. 13, 2012), https://techtalk.gfi.com/security-patching-trends-for-major-software-vendors/.

II. OVERVIEW OF VULNERABILITY MANAGEMENT AND PATCH MANAGEMENT

Most computer users are familiar with software updates. Whether it is an update for the operating system on a Windows computer or an iPhone, the update fixes bugs or vulnerabilities in the software.[28] In a business setting, the employees who use a laptop to carry out their duties, also called "end users," are generally unaware of the various software on the company's network and the updates. The responsibility for identifying the software that needs to be updated, prioritizing the updates, and implementing the updates usually falls to the information technology and information security teams.[29] The technical terms for these processes are vulnerability management and patch management.[30] A non-technical overview of the tools used for these processes are explained below.

A. Vulnerability Management

The processes by which vulnerabilities are identified are varied. Every day, computer security researchers[31] examine software for problems in the computer code that cause the software to do something it is not intended to do.[32] These weaknesses, or vulnerabilities, in the software could be exploited by an attacker to perform an unauthorized action within a computer system.[33] Ideally, before publicly disclosing the vulnerability, the computer security researcher notifies the software vendor about the vulnerability and gives the vendor an opportunity to create a "patch" that fixes the vulnerability.[34] Once the vulnerability has been publicly disclosed,

---

28. *See Understanding Patches and Software Updates*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://us-cert.cisa.gov/ncas/tips/ST04-006 (Nov. 19, 2019).

29. Armerding, *supra* note 23.

30. This article addresses vulnerabilities in software and the application of patches to mitigate those vulnerabilities. Others use the term "vulnerability management" to broadly refer to a variety of weaknesses including mismanagement of IT hardware and software or even physical security issues. *See, e.g.*, Sean Atkinson, *Cybersecurity Tech Basics: Vulnerability Management: Overview*, THOMSON REUTERS (2018), https://www.cisecurity.org/wp-content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf.

31. Software companies employ security researchers and others to identify vulnerabilities in their software. For example, these researchers may examine the code within malware in circulation in order to determine whether malware can be used to exploit a previously unknown vulnerability within software. Independent security researchers who work for security firms unaffiliated with software companies similarly investigate and identify these vulnerabilities.

32. Atkinson, *supra* note 30, at 1.

33. *Id.*

34. Vulnerability disclosure best practices are discussed in Allen D. Householder et al., *The CERT Guide to Coordinated Vulnerability Disclosure*, CARNEGIE MELLON UNIV.:

the Mitre Corporation (MITRE), a federally funded research center, assigns the vulnerability a unique Common Vulnerability Enumeration (CVE),[35] and the National Institute of Standards and Technology (NIST) publishes information about the vulnerability in the National Vulnerability Database (NVD).[36] Within an organization, the IT team or information security team is responsible for reviewing the software on the organization's network to identify, classify, remediate, and mitigate the software vulnerabilities.[37] The process of "identifying, classifying, remediating, and mitigating vulnerabilities" is called vulnerability management.[38]

There are several different ways an IT team can become aware of a newly identified software vulnerability. One typical way is through email notifications directly from the software vendor.[39] Typically, the IT team signs up for these notifications based on the software the business is running.[40] Another typical way is through the use of software—vulnerability scanners—to "scan" systems and networks for hosts using outdated or unsupported software.[41] A "host" includes servers, desktop personal computers, or personal electronic devices.[42] The vulnerability scanners generate a report that identifies the total number of identified hosts and vulnerabilities, including a risk level for each vulnerability.[43] In addition to identifying software vulnerabilities that require patching, the results from the vulnerability scanners can identify vulnerabilities

---

SOFTWARE ENG'G INST. (Aug. 2017), https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

35. *About CVE*, COMMON VULNERABILITIES & EXPOSURES, https://cve.mitre.org/about/index.html (Mar. 29, 2021).

36. *National Vulnerability Database: Statistics Results*, *supra* note 17.

37. *See generally* Tom Palmaers, *Implementing a Vulnerability Management Process*, GLOB. INFO. ASSURANCE CERTIFICATION (Mar. 23, 2013), https://www.giac.org/paper/gsec/32851/implementing-vulnerability-management-process/112555.

38. PARK FOREMAN, VULNERABILITY MANAGEMENT 1 (2d ed. 2019).

39. *See, e.g.*, *Adobe Security Notifications Registration: Security Notification Service*, ADOBE, https://www.adobe.com/subscription/adbeSecurityNotifications.html (last visited Feb. 11, 2021).

40. *See, e.g.*, *id.*

41. Common vulnerability scanning software vendors include Tenable, Qualys, Rapid7, and Nexpose. *See, e.g.*, *Close Your Cyber-Exposure Gap*, TENABLE, https://www.tenable.com/products (last visited Mar. 10, 2021); *Nexpose Vulnerability Scanner*, RAPID7, https://www.rapid7.com/products/nexpose/ (last visited Mar. 10, 2021); *Vulnerability Management That's Accurate and Scales!*, QUALYS, https://www.qualys.com/lp/vulnerability-management/ (last visited Mar. 10, 2021).

42. Miles Tracy et al., *Guidelines on Securing Public Web Servers: Recommendations of the National Institute of Standards and Technology*, NAT'L INST. STANDARDS & TECH. app. B, at B-1 (Sept. 2007), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf.

43. *See, e.g.*, Warlock, *Vulnerability Assessment with Nexpose*, INFOSEC RES. (Dec. 27, 2013), https://resources.infosecinstitute.com/topic/vulnerability-assessment-nexpose/.

due to configuration problems or outdated certificates.[44] While these are vulnerabilities that the IT and information security teams should address, they are separate from vulnerabilities that require patching.

Traditionally, vulnerability scanners were "agentless," but agent-based scanning is also now available.[45] In addition to the decision about whether to use agentless scanning, agent-based scanning, or both, the IT and information security teams must decide how often to scan and what to scan.[46] Agentless scanning and agent-based scanning offer different features for identifying vulnerabilities which are explained below.

1. Agentless Scanning

Agentless scanning relies on one or more servers to perform network scanning of each host. The scan collects information about the host, including what versions of different software the host is running.[47] Agentless scanning can be "credentialed" or "non-credentialed."[48] Credentialed scanning requires that the IT team enter an administrator username and password into the scanning application.[49] The application then has greater access to the host to return more accurate scanning results. In a given network, there is likely more than one set of administrator credentials. The process of ensuring the scanning application has the correct administrator credentials can be burdensome. The analogies for the difference between "credentialed" or "non-credentialed" are many, including the difference between an x-ray and an MRI or a home inspection conducted from the sidewalk versus going inside the home.[50]

The scope of agentless scanning is limited to hosts on the local network. This means laptops and mobile devices not on the network during the scan are omitted from the results.[51] Other

---

44. Atkinson, *supra* note 30.

45. *See* Murugiah Souppaya & Karen Scarfone, *Guide to Enterprise Patch Management Technologies*, NAT'L INST. STANDARDS & TECH. 8 (July 2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.

46. *See id.*

47. *Id.*

48. This is also referred to as "authenticated" or "unauthenticated" scanning. *See* Lucian Constantin, *What Are Vulnerability Scanners and How Do They Work?*, CSO ONLINE (Apr. 10, 2020, 3:00 AM), https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html.

49. *Id.* Because the administrator password can be intercepted, some IT teams use keys or certificates for credentialed scans.

50. *See, e.g.*, Lascon, *Vulnerability Management: You're Doing It Wrong*, YOUTUBE (Jan. 21, 2019), https://youtu.be/yUZ_YFSNQQE (referencing material at time stamp 19:30).

51. Souppaya & Scarfone, *supra* note 45, at 9.

limitations of agentless scanning include other security controls that may inadvertently block the scanning and considerations due to the scanning consuming excessive amounts of bandwidth.[52]

2. Agent-Based

Unlike agentless scanning, agent-based scanning requires the installation of software, an "agent," on each host. The agent has administrator privileges, which ensures every scan is "credentialed." The agent sends the information back to a server that collects information about the host including what versions of software the host is running. Unlike agentless scanning, agent-based scanning is not dependent on the host being on the corporate network.

B. Patch Management

The scale of correctly and safely implementing a patch across an entire organization can be challenging. Prior to releasing a patch, software vendors test the patch to ensure the software continues to properly function. However, it is not possible for the software vendor to test how every application or third-party software will react to the patch. This task is left to IT departments. Typically, the IT department tests the patch in a test environment to see whether it causes other applications to perform in unexpected ways, including causing other applications to crash or run slowly. After testing the patched software, the IT department will decide to install the patch or not. In some cases, companies have found it prudent to delay the installation of a patch while awaiting any report of security issues related to the patch itself. If the IT department installs the patch, the final step in the process is verifying the installation. This resource intensive process of "identifying, acquiring, installing, and verifying patches for products and systems" is called patch management.[53]

Because the process is resource intensive, IT departments must make decisions about how to optimally patch the vulnerabilities that pose the greatest risk to the organization. Typically, the process is formalized in a patch management process or procedure and may include a service-level agreement (SLA) between the IT and information security teams. The process, procedure, and SLA can vary in terms of the level of detail it contains, including the length of time available for the IT department to patch vulnerabilities

52. *Id.*
53. *Id.* at 2.

based on severity rating, *e.g.*, critical vulnerabilities must be patched within one week.[54]

Organizations typically consider the following characteristics when making decisions about which vulnerabilities to prioritize.

1. Severity Based on CVSS

The CVSS is a de facto international standard for measuring the severity of a vulnerability.[55] The CVSS score uses eight characteristics of a vulnerability to produce a numeric score between zero and ten, which corresponds to a severity rating: low (0.1–3.9), medium (4.0–6.9), high (7.0–8.9), and critical (9.0–10.0).[56] As explained above, the severity of the EternalBlue vulnerabilities used in the NotPetya and WannaCry malware was "high." One of the EternalBlue vulnerabilities was CVE-2017-0143. The numeric score for the vulnerability was 8.1. As an example of the CVSS rating, the eight characteristics for the vulnerability and a brief explanation of the applicable characteristic are as follows:

- Attack Vector—Network. The vulnerability can be executed remotely.
- Attack Complexity—High. A successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation before a successful attack can be expected.
- Privileges Required—None. The attacker does not require any prior access to settings or files to carry out the attack.
- User Interaction—None. The vulnerable system can be exploited without any interaction by a user. For example, it does not require a user to open a file or click on something.
- Scope—Unchanged. The exploited vulnerability can only affect systems managed by the same authority.
- Confidentiality—High. The attacker is able to divulge all the resources within the impacted system.
- Integrity—High. The attacker is able to modify all files protected by the impacted system.

---

54. When an SLA identifies required due dates for different vulnerabilities based on severity, the SLA due dates may have to account for situations where a CVE does not have a patch immediately available.

55. Jay Jacobs et al., *Improving Vulnerability Remediation Through Better Exploit Prediction*, J. CYBERSECURITY, July 17, 2020, at 4.

56. *National Vulnerability Database: Vulnerability Metrics*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/vuln-metrics/cvss (last visited Feb. 12, 2021).

- Availability—High. The attacker is able to fully deny access to resources in the impacted system.

One common approach to patch management is to prioritize patches based on the CVSS score.[57] For internet-accessible systems, the Department of Homeland Security requires federal agencies remediate critical vulnerabilities within fifteen calendar days of initial detection and high vulnerabilities within thirty calendar days of initial detection.[58] Similarly, the Payment Card Industry Data Security Standard (PCI-DSS) contains a requirement that no medium, high, or critical vulnerabilities be present on internet-accessible systems within the payment card environment, absent compensating controls.[59]

Even if an organization limits its patch management to critical and high vulnerabilities, the number of vulnerabilities can be overwhelming. Between 2017 and 2020, there were more than 4,000 critical and high vulnerabilities reported by US-CERT each year.[60]

2. Availability and Use of an Exploit

A different approach to patch management focuses on whether attackers have exploited the vulnerability or whether an exploit is available. A vulnerability is only a weakness in particular software.[61] In order for an attacker to exploit the vulnerability, the attacker needs a written exploit—software code that takes advantage of the vulnerability. Of the thousands of vulnerabilities identified in software every year, written exploits are available for only a small percentage.[62] An even smaller number of exploits are

---

57. Jacobs et al., *supra* note 55, at 6.

58. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., BINDING OPERATIONAL DIRECTIVE 19-02, VULNERABILITY REMEDIATION REQUIREMENTS FOR INTERNET-ACCESSIBLE SYSTEMS (2019) (available at https://cyber.dhs.gov/assets/report/bod-19-02.pdf).

59. PAYMENT CARD INDUS. DATA SEC. STANDARD, REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 99 (May 2018) (Requirement 11.2.2–11.2.3).

60. *National Vulnerability Database: CVSS Severity Distribution over Time*, NAT'L INST. STANDARDS & TECH., https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time (last visited Feb. 12, 2021). The chart relies on CVSS V2 scores, instead of the current CVSS V3. *See id.* Under CVSS V2, a numeric value of seven or greater was a high severity vulnerability. *Id.* CVSS V3 added an additional severity level of critical for numeric values of nine or greater. *Id.*

61. Gary Stoneburner et al., *Risk Management Guide for Information Technology Systems*, NAT'L INST. STANDARDS & TECH. 15 (July 2002), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf.

62. MEHRAN BOZORGI ET AL., BEYOND HEURISTICS: LEARNING TO CLASSIFY VULNERABILITIES AND PREDICT EXPLOITS (2010), https://cseweb.ucsd.edu/~saul/papers/kdd10_exploit.pdf (estimating written exploits are available for 10–15% of vulnerabilities); Jacobs et al., *supra* note 55, at 5 (estimating written exploits are available for approximately 12% of vulnerabilities).

actually used to target corporate networks.[63] One approach suggested by security researchers is to prioritize patching based on whether a published exploit is available.[64]

3. Characteristics of the System

A third consideration for determining which systems to patch is the characteristics of the system. Important characteristics include whether or not the system is internet facing and how critical the system is to the business. A system that is internet facing is more vulnerable to exploitation because an attacker does not need to be on the same network to exploit the vulnerability. The criticality of the system to the business is important because critical systems should be prioritized for patching.

C. Other Compensating Controls

Sometimes patching a piece of software is not practical because it would be too disruptive to the organization. Some older systems may be "fragile" and critical to the business. Because the system is fragile, patching the system may break the critical application or service. Other operating systems may not be able to be patched because they have applications that do not work with newer versions of the operating system. This can occur when a version of Microsoft Windows reaches its end of life. For example, Microsoft stopped supporting Windows 7 in January 2020, and it will end support for Windows 10 in May 2021.[65]

When this occurs, the IT and information security teams will typically rely on other techniques, or "compensating controls," to reduce the risk that the vulnerability will be exploited. The other techniques can include increasing logging and monitoring on the unpatched systems or reducing accessibility to the system through

63. CARL SABOTTKE ET AL., VULNERABILITY DISCLOSURE IN THE AGE OF SOCIAL MEDIA: EXPLOITING TWITTER FOR PREDICTING REAL-WORLD EXPLOITS (2015), https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sabottke.pdf (observing exploits in the wild for 1.3% of vulnerabilities); Jacobs et al., *supra* note 55, at 2 (observing exploits in the wild for 5.5% of vulnerabilities).

64. Jacobs et al., *supra* note 55, at 10 ("For example, if a firm addresses vulnerabilities that have a proof-of-concept code published in Exploit DB, our model will achieve a comparable level of coverage, '*but at one-quarter the level of effort*.'") (emphasis added).

65. *Products Ending Support in 2021*, MICROSOFT, https://docs.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2021 (Mar. 11, 2021); *Support for Windows 7 Has Ended*, MICROSOFT, https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-7-support (last visited Feb. 12, 2021).

an "allow list."[66] An allow list is a list of IP addresses that are permitted to access the unpatched system.

III. OVERVIEW OF SECURITY STANDARDS RELATING TO VULNERABILITY AND PATCH MANAGEMENT

Like many other technical areas of responsibility, non-profit organizations and government agencies provide technical standards to guide information security professionals. The standards address a wide range of security concepts and establish "best practices" for different aspects of a comprehensive information security program. All of the leading security standards now reference vulnerability management and patch management. The leading security standards include the National Institute of Standards and Technology (NIST), Center for Internet Security's Critical Security Controls, International Organization for Standardization (ISO) 27000 standards, and PCI-DSS. These standards have been endorsed by the California Attorney General's Office and the Ohio Data Protection Act.[67] An overview of the leading security standards and their references to vulnerability management and patch management are provided below.

A. NIST

NIST is an agency of the United States Department of Commerce that functions as the "lead national laboratory for providing the measurements, calibrations, and quality assurance techniques which underpin United States commerce, technological progress, improved product reliability and manufacturing processes, and public safety."[68] In 2014, Congress amended the National Institute of Standards and Technology Act and directed NIST to develop a "voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to

66. Katie Stewart, *Establish and Maintain Whitelists (Part 5 of 7: Mitigating Risks of Unsupported Operating Systems)*, CARNEGIE MELLON UNIV.: SOFTWARE ENG'G INST. (Oct. 25, 2017), https://insights.sei.cmu.edu/insider-threat/2017/10/establish-and-maintain-whitelists-part-5-of-7-mitigating-risks-of-unsupported-operating-systems.html. The term whitelist is also known as "allow list." Emma W, *Terminology: It's Not Black and White*, NAT'L CYBER SEC. CTR. (Apr. 30, 2020), https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white. Many organizations, including the United Kingdom's National Cyber Security Centre, have stopped using the term "whitelist" and use "allow list" instead. *Id.*

67. *See* KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 2012–2015, at 30 (Feb. 2016) (available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf); *see also* Ohio Data Protection Act, OHIO REV. CODE ANN. §§ 1354.01–1354.05.

68. 15 U.S.C. § 271(b)(1).

cost-effectively reduce cyber risks to critical infrastructure."[69] The same year, NIST published version 1.0 of the NIST Cybersecurity Framework.[70] In April 2018, NIST published version 1.1, the current version of the NIST Cybersecurity Framework (NIST Framework).[71] The NIST Framework identifies five core "functions" for cybersecurity and matches each function with a subcategory and an informative reference for existing standards and guidelines.[72] The following subcategories notably identify and address vulnerability management and patch management as part of these best practices:

- DE.CM-8: Vulnerability scans are performed.
- ID.RA-1: Asset vulnerabilities are identified and documented.

Another relevant NIST publication is NIST's flagship information security publication, Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, which provides a catalog of security and privacy controls for information systems and organizations.[73] In this document, two controls relevant to vulnerability management and patch management are set forth: Control RA-5, Vulnerability Monitoring and Scanning, cites monitoring and scanning for vulnerabilities in the system at a frequency defined by the organization,[74] while Control SI-2, Flaw Remediation, recommends that organizations test software updates then install "security-relevant" software updates within an "organization-defined time period" after release of the update.[75]

B. Center for Internet Security Controls

The Center for Internet Security (CIS) is a nonprofit organization whose mission is "to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves

69. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

70. *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*, NAT'L INST. STANDARDS & TECH. (Feb. 12, 2014), https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

71. *See Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*, NAT'L INST. STANDARDS & TECH. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

72. *Id.* at 6–7.

73. *See generally* Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, NAT'L INST. STANDARDS & TECH. (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

74. *Id.* at 269.

75. *Id.* at 333.

against pervasive cyber threats."[76] Similar to NIST, CIS has developed the "CIS Controls," a set of twenty security controls.[77] Among the six priority controls, referred to as the "Basic CIS Controls," is CIS Control 3: "Continuous Vulnerability Management."[78] The subcontrols for CIS Control 3 address the specific requirements to implement the control:

- CIS Control 3.1: Run Automated Vulnerability Scanning Tools
- CIS Control 3.2: Perform Authenticated Vulnerability Scanning
- CIS Control 3.3: Protect Dedicated Assessment Accounts
- CIS Control 3.4: Deploy Automated Operating System Patch Management Tools
- CIS Control 3.5: Deploy Automated Software Patch Management Tools
- CIS Control 3.6: Compare Back-to-back Vulnerability Scans
- CIS Control 3.7: Utilize a Risk-rating Process

Additionally, CIS Control 18.8, relating to Application Software Security, requires that organizations "[e]stablish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact [the organization's] security group."[79]

C. ISO

The ISO is an international organization that publishes standards for different industries, including information security.[80] The ISO 27000 standards series, which are published jointly by the ISO and the International Electrotechnical Commission (IEC), is meant to provide best practices for information security management.[81]

---

76. *About Us*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/about-us/ (last visited Feb. 13, 2021).

77. *CIS Controls Navigator*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-implementation-groups/ (last visited Feb. 13, 2021).

78. *Continuous Vulnerability Management*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/continuous-vulnerability-management/ (last visited Feb. 13, 2021).

79. *18.8: Establish a Process to Accept and Address Reports of Software Vulnerabilities*, CONTROLS ASSESSMENT SPECIFICATION, https://controls-assessment-specification.readthedocs.io/en/latest/control-18/control-18.8.html (last visited Feb. 13, 2021).

80. *See generally Standards*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/standards.html (last visited Jan. 18, 2021).

81. ISO/IEC 27001:2013(en), INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (last visited Mar. 1, 2021). This version was reviewed and confirmed in 2019. ISO/IEC 27001:2013, INT'L ORG. FOR STANDARDIZATION (Oct. 2013), https://www.iso.org/standard/54534.html.

Organizations that adopt and implement ISO 27000 can hire third-party auditors to certify the company as compliant with different standards that are part of the series. A common standard for certification is ISO 27001.[82] The next standard in the series, ISO 27002, provides a reference for organizations implementing ISO 27001. One of the controls, or measures taken to reduce information security risks, identified in ISO 27002 is control A.12.6—Technical vulnerability management.[83] This control requires that "[i]nformation about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk."[84] A series of other steps and implementation guidance includes maintaining an accurate inventory of assets on the network, identifying roles and responsibilities for members of the organization who support vulnerability management, creating a timeline for the process, and analyzing the risks for implementing a patch.

D. PCI-DSS

The PCI-DSS is a standard promulgated by the payment card industry that applies to the various entities that process payment cards—merchants, processors, service providers, and banks.[85] First released in 2004 and updated periodically, the standard sets a baseline of technical and operational requirements that the payment card brands direct entities to follow. The current version requires organizations to scan for internal and external security vulnerabilities and patch or mitigate them. In addition, PCI-DSS explicitly requires the minimum frequency for scanning, the time in which patches must be applied, and the risk rating score for patching:

- Requirement 6.1: Establish a process to identify security vulnerabilities using reputable outside sources for security vulnerability information and assign a risk ranking (for example as "high" "medium" or "low") to newly discovered security vulnerabilities.
- Requirement 6.2: Ensure that all system components and software are protected from known vulnerabilities by

82. ISO/IEC 27002:2013, INT'L ORG. FOR STANDARDIZATION (Oct. 2013), https://www.iso.org/standard/54533.html.

83. *Id.*

84. *Id.*

85. *About Us*, PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ (last visited Feb. 14, 2021).

installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

- Requirement 11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations changes in network topology firewall rule modifications product upgrades).
- Requirement 11.2.1: Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.
- Requirement 11.2.2: Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

IV. LEGAL RISKS

Following a data breach, the victim organization can face regulatory investigations and enforcement actions, as well as civil litigation, often in the form of class actions.[86] The potential legal liability depends on a variety of factors, including the data the attacker accesses or acquires and what the company did to protect itself and its data. A review of regulatory enforcement actions and guidance, as well as evolving case law, reveal that issues relating to vulnerability and patch management have been recognized as the basis for liability.

A. Regulators

A variety of state and federal regulators take the position that they have jurisdiction to bring legal action against a company in response to a breach. Specific industry regulators may have enforcement authority under statutes that apply to particular industries. For example, the Federal Trade Commission (FTC) enforces the Federal Trade Commission Act (FTCA) (in the context of consumer protection) and the Gramm-Leach-Bliley Act (GLBA) (in the

86. This article does not address legal implications under contract law or foreign legal requirements. Both should also be considered and may impose additional legal risks.

context of financial institutions), the Department of Health and Human Services Office of Civil Rights (HHS OCR) enforces the Health Insurance Portability and Accountability Act (HIPAA), and the Securities and Exchange Commission (SEC) enforces the Safeguards Rule of Regulation S-P. Beginning with an enforcement action against Guess? and through publications about information security,[87] the FTC has indicated that effective vulnerability management and patch management are important considerations in its determination of whether companies, including vendors, have "reasonable" information security practices. HHS OCR has similarly indicated that it considers vulnerability management and vulnerability management to be important parts of an information security program. The SEC has not brought an enforcement action for failure to implement vulnerability management and risk management, but it has discussed the importance of them in publications.

1. Federal Trade Commission

The FTC is an independent federal agency aimed at protecting consumers and competition.[88] Through enforcement, education, and advocacy, it protects consumers from unfair and deceptive practices in vast sectors of the economy.[89] The FTC brings a variety of enforcement actions, addressing an array of issues. Relevant to information security are the FTC's enforcement actions under both the "deceptiveness" and "unfairness" prongs of Section 5 of the FTC Act and the Safeguards Rule under the GLBA.[90] In recent enforcement actions and in official publications, the FTC has demonstrated a growing interest in vulnerability management and patch management.

a. Enforcement Under the FTCA

Purporting to act under its authority to prevent "unfair" practices in commerce, the FTC has brought enforcement actions against companies for a failure to implement reasonable cybersecurity measures. While the existence and scope of that jurisdiction continues to be debated, in *FTC v. Wyndham Worldwide Corporation*,

87. Guess?, Inc., 136 F.T.C. 507, 511 (2003) (Complaint) (FTC alleged Guess? failed "to implement reasonable and appropriate measures to secure and protect the databases that support or connect to the website" by failing to "test or otherwise assess the website's or the application's vulnerability to attacks . . . .").

88. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Dec. 28, 2020).

89. *Id.*

90. 15 U.S.C. § 45(a)(1); 16 C.F.R. §§ 314.1–314.5 (2002).

the Court of Appeals for the Third Circuit affirmed the FTC's authority to regulate cybersecurity under the unfairness prong of Title 15 U.S.C. Section 45(a).[91] This decision has been criticized on a number of grounds, including because the FTC failed to provide notice to companies about what constitutes "reasonable" information security practices.[92] In *FTC v. Wyndham Worldwide Corporation*, the Third Circuit held that fair notice is satisfied when a company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.[93] The court observed that the relevant inquiry under subsection 45(n) for unreasonableness is a cost-benefit analysis that considers "the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[94]

In the *Wyndham* case, the FTC alleged that hackers attacked the Wyndham Corporation's computer systems in three separate incidents in 2008 and 2009, stealing hundreds of thousands of consumers' PII and leading to over $10 million in fraudulent charges.[95] Following the attacks, the FTC filed suit in federal district court alleging Wyndham engaged in "unfair cybersecurity practices" and the corporation "unreasonably and unnecessarily exposed consumers" PII to attack.[96] The FTC alleged Wyndham "permitt[ed] Wyndham-branded hotels 'to connect insecure servers to [h]otels and [r]esorts' networks, including servers using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities.'"[97] This is one of many complaints by the FTC that allege a company did not have "reasonable" information security practices, in part, due to unpatched or unsupported software.

---

91. 799 F.3d 236, 240 (3d Cir. 2015). Relevant here, one of the charges against Wyndham, involved insufficient patch management on network connect computers. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014).

92. *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 719 (2013); *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 183 (2008). *See generally* Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standardless Data Security Standard*, 15 J.L. ECON. & POL'Y 67 (2019). *See also* LabMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018) (ruling FTC cease and desist order was unenforceable due to vagueness of requirement of "reasonably designed data-security program").

93. *Wyndham Worldwide Corp.*, 799 F.3d at 256.

94. *Id.* at 255.

95. *Id.* at 240.

96. *Id.*

97. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014).

Although not directed at internal vulnerability management and patch management programs, two FTC enforcement actions against software and hardware vendors for their alleged failure to provide proper software updates to their customers demonstrate the FTC's consideration of the importance of software updates. In 2011, the FTC brought an enforcement action against Oracle due in part to software updates to Java, a programming language that Oracle had developed.[98] The FTC alleged that Oracle knew that its consumers were vulnerable to attack due to Java's insufficient update process.[99] The FTC cited internal Oracle documents stating that the "Java update mechanism is not aggressive enough or simply not working."[100] The FTC alleged when Java consumers updated the Java software, unbeknownst to the consumers, prior versions of the software remained on the consumers' computers.[101] The FTC claimed that hackers exploited the flaw and accessed consumers' data through the outdated Java versions.[102] In the consent agreement, the FTC ordered Oracle to improve the Java updating process and conspicuously inform consumers of the versions of Java installed on their devices.[103]

In 2016, the FTC brought a similar action against ASUSTeK Computer, Inc. (ASUS) for its alleged failure to protect users of ASUS's routers from cyberattack.[104] ASUS, a hardware manufacturer, developed software for its routers and was responsible for developing and distributing software updates to patch security vulnerabilities.[105] Many of ASUS's routers included features called AiCloud and AiDisk, which allowed consumers to plug USB hard drives directly into the routers to create an at-home "private personal cloud."[106] In 2014, hackers exploited vulnerabilities in AiCloud and accessed over 12,900 consumers' storage devices.[107] The FTC alleged hackers accessed the users' connected storage devices without credentials by bypassing the AiCloud login screen.[108] Additionally, the FTC alleged the default settings on AiDisk made

98. Oracle Corp., No. 132-3115, 2015 WL 9412609, at *1 (F.T.C. Dec. 21, 2015) (Complaint).
99. *Id.*
100. *Id.* at *2.
101. *Id.*
102. *Id.* at *3.
103. *Id.* at *6–7 (Order).
104. ASUSTeK Comput., Inc., No. 142-3156, 2016 WL 4128217, at *1 (F.T.C. July 18, 2016) (Complaint).
105. *Id.*
106. *Id.* at *2.
107. *Id.*
108. *Id.*

the storage devices accessible to anyone on the internet who had the routers' IP addresses.[109] The FTC alleged that ASUS did not notify consumers about available security updates.[110] Moreover, the tool that informed consumers of available security updates often told consumers their software was up-to-date when, in fact, newer software with "critical security updates" was available.[111] The FTC ordered ASUS to establish a comprehensive security program.[112] Specifically, the FTC ordered ASUS to notify consumers about software updates and to refrain from making misleading statements regarding whether consumers' products were up-to-date.[113]

In recent consent decrees, the FTC has consistently ordered companies to implement patch management programs.[114] In 2020, the number of people who participated in Zoom meetings each day rose from approximately 10 million to 300 million.[115] Within this context, the FTC claimed Zoom undermined the security of its users by engaging in unfair and deceptive trade practices.[116] According to the FTC, Zoom had failed to maintain proper internal network security, despite touting its advanced security practices.[117] Relevant here, the FTC alleged Zoom was a year or more behind in patching software in its commercial environment.[118] As part of its settlement with the FTC—in addition to discontinuing some of the practices alleged in the complaint—Zoom must implement specific security safeguards, including conducting vulnerability scans on at least a quarterly basis and implementing policies and procedures to remediate critical or high vulnerabilities no later than thirty days after detection.[119] Zoom must hire a third party to conduct an

109. *Id.* at *3.
110. *Id.* at *4.
111. *Id.* at *6.
112. *Id.* at *13–15 (Order).
113. *Id.* at *14.
114. Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FED. TRADE COMM'N: BUS. BLOG (Jan. 6, 2020, 9:46 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance ("We were also mindful of the 11th Circuit's 2018 LabMD decision, which struck down an FTC data security order as unenforceably vague. Based on this learning, in 2019 the FTC made significant improvements to its data security orders.").
115. Zoom Video Commc'ns, Inc., No. 192-3167, 2020 WL 6589815, at *2 (F.T.C. Nov. 9, 2020) (Complaint).
116. *Id.* at *2–3.
117. *Id.* at *3.
118. *Id.*
119. Zoom Video Commc'ns, Inc., No. 192-3167, 2020 WL 6589819, at *1–3 (F.T.C. Nov. 9, 2020) (Analysis of Proposed Consent Order to Aid Public Comment).

independent assessment of the new safeguards once every other year for twenty years.[120]

Moreover, in post-2018 cases, involving SkyMed, D-Link, and InfoTrax, the FTC ordered companies to implement security safeguards that include vulnerability testing.[121] For example, it ordered InfoTrax to scan for vulnerabilities every four months.[122]

The consent agreement in Zoom and agreements in other recent cases exemplify the FTC's recent specific focus on ordering entities to implement vulnerability management programs. The requirement to implement a vulnerability management program is more specific than previous orders, which at times vaguely required companies to implement reasonable security programs "designed to protect the security . . . of personal information . . . ."[123] The more recent orders are still broad and susceptible to a wide range of interpretations, and ultimately, companies face potential legal risk as they try to navigate the logistical and practical challenges of prioritizing which out-of-date software to update.

b. Enforcement Under the GLBA

While the FTC has brought enforcement actions for violation of the GLBA Safeguards Rule, the complaints and consent orders have not explicitly referenced vulnerability management and patch management. The Safeguards Rule, which implements section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions develop a written information security program that contains "administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[124] The Safeguards Rule identifies general requirements. Influenced by the New York Department of Financial Services (NY DFS) Cybersecurity Requirements for Financial Services Companies, the FTC has proposed a revised Safeguards Rule that contains more specific information security requirements.[125] Although the proposed revision does not explicitly reference vulnerability management and patch management, it does reference periodic vulnerability

120. *Id.* at *2–3.

121. Skymed Int'l, Inc., No. 192-3140, 2020 WL 7646326, at *4 (F.T.C. Dec. 16, 2020); FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD (N.D. Cal. Sept. 19, 2017) (Leagle); InfoTrax Sys., L.C., No. 162-3130, 2019 WL 6168270, at *3 (F.T.C. Nov. 12, 2019).

122. *InfoTrax Sys., L.C.*, 2019 WL 6168270, at *3.

123. LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018).

124. 16 C.F.R. § 314.1 (2002).

125. *See* Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (Apr. 4, 2019).

assessments.[126] Neither the proposed revisions nor the NY DFS regulations define vulnerability assessments.

c. FTC Publications

The FTC has issued a number of publications addressing what it considers reasonable for vulnerability management and patch management. In the FTC brochure, *Start with Security*, the FTC explains the need for patch management programs stating:

> [d]epending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.[127]

In 2016, the FTC recommended that entities, as part of their general network security, regularly check with vendors and experts for alerts about vulnerabilities and "implement policies for installing vendor-approved patches to correct problems."[128] Then in 2020, the FTC reiterated its requirement for patch management programs, explaining that its recent consent decrees had ordered companies to implement such programs.[129]

Together, the orders and publication suggest that the FTC believes that patch management programs are fundamental to reasonable cybersecurity but also that the agency understands that it is not a one-size-fits-all process. As explained in Section II, the adequacy of vulnerability management and patch management remains a question of degree. For many companies, it is cost prohibitive to patch every out-of-date software on every system. Instead, companies prioritize based on risk calculations. Thus, vulnerability management and patch management are unlike some other areas of information security, which can be binary, *e.g.*, customer files are encrypted or they are not, default passwords must be changed or they are not. The exceptions to this general observation are when a company has internal policies or makes statements that a third party or the public relies on about its vulnerability management and patch management programs that it fails to follow. Setting

126. *Id.* at 13,176.

127. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 12 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

128. FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 10 (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

129. Smith, *supra* note 114.

these exceptions aside, in the wake of this ambivalent guidance, a company needs to make decisions about what is reasonable, and they may not be the same decisions the FTC would have made.

2. U.S. Department of Health and Human Services Office for Civil Rights (HHS OCR)

Like the FTC, the HHS OCR has also demonstrated an interest in investigating and bringing enforcement actions for vulnerability management and patch management practices.[130] HHS OCR enforces the implementing regulations under HIPAA and the HITECH Act of 2009.[131] The applicable regulations for information security are the Privacy Rule[132] and the Security Rule.[133] Entities subject to the regulations ("covered entities") include certain healthcare providers, health plans, and healthcare clearinghouses.[134] Business associates of covered entities are also subject to certain regulatory oversight by HHS OCR.[135] This includes any person or organization that performs services for a covered entity that includes the use of or disclosure of protected health information (PHI).[136]

The Security Rule requires covered entities and business associates to protect electronic PHI (ePHI) and establishes minimum security requirements to do so.[137] The Security Rule consists of "standards" and "implementation specifications." Some of the standards are required, while others are considered "addressable." Although the Security Rule does not reference vulnerability management or patch management, covered entities and business associates are required under the rule to conduct a "risk analysis," implement a "risk management" process, and ensure "transmission

130. *See* Resolution Agreement between HHS OCR and Anchorage Community Mental Health Services, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 2, 2014), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf.

131. OCR, *About Us*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Oct. 8, 2019), https://www.hhs.gov/ocr/about-us/index.html; OCR, *HITECH Act Rulemaking and Implementation Update*, U.S. DEP'T OF HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/security/guidance/hitech-act-rulemakingimplementation-update/index.html.

132. 45 C.F.R. pt. 160 (2013); 45 C.F.R. §§ 164.102–164.106 (2013); 45 C.F.R. §§ 164.302–164.318 (2013).

133. 45 C.F.R. pt. 160, 164.

134. 45 C.F.R. § 160.103 (2014).

135. *Id.*

136. *Id.*

137. *Id.* ePHI is defined as protected health information that is transmitted by electronic media or maintained in electronic media. *Id.*

security."[138] This process likely will include evaluations of a company's vulnerability and patch management.

A risk analysis is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI a covered entity or business associate holds.[139] Under the Security Rule, the risk management process implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.[140] According to an HHS OCR newsletter from July 2018, a risk analysis includes identifying risks and vulnerabilities that unpatched software poses to an organization's ePHI.[141] In the July 2018 newsletter, HHS OCR stated that implementing security measures can include "installing patches if patches are available and patching is reasonable and appropriate."[142]

Failures to adequately address vulnerabilities have also been explicitly cited in HHS OCR enforcement actions. In a settlement announced in 2014, HHS OCR stated that a covered entity suffered a breach of unsecured ePHI due to the covered entity's failure to regularly update its "IT resources with available patches."[143] The settlement agreement[144] indicated that the failure to update IT resources with available patches was a violation of the transmission security requirement of the Security Rule.[145]

As such, HHS OCR clearly considers vulnerability management and patch management as important requirements for covered entities and business associates. However, the 2018 newsletter indicates that HHS OCR may take a potentially flexible approach to evaluating patch management through an understanding that deployment of a patch may not be appropriate. In those cases, HHS OCR likely expects that entities implement compensating controls

138. 45 C.F.R. §§ 164.308(a)(1)(ii)(A)–(B); *id.* § 164.312(e)(1).

139. *Id.* § 164.308(a)(1)(ii)(A).

140. *Id.* § 164.308(a)(1)(ii)(B).

141. *Guidance on Software Vulnerabilities and Patching*, U.S DEP'T OF HEALTH & HUM. SERVS. OFF. FOR C.R. 1 (June 2018), https://www.hhs.gov/sites/default/files/june-2018-newsletter-software-patches.pdf.

142. *Id.* at 2.

143. *Bulletin: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software*, U.S DEP'T OF HEALTH & HUM. SERVS. OFF. FOR C.R. 1 (Dec. 2014), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf.

144. *See* Resolution Agreement, *supra* note 130.

145. The Security Rule requires "transmission security" which are "technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network." 45 C.F.R. § 164.312(e)(1) (2013).

to reduce the risk of identified vulnerabilities in the unpatched software.[146]

3. The Securities and Exchange Commission

The SEC enforces a variety of different statutes and regulations, including the Safeguards Rule of Regulation S-P, which requires that brokers, dealers, investment companies, and registered investment advisors adopt written policies and procedures reasonably designed to protect customer records and information.[147] In the cases where the SEC has brought enforcement actions for violations of the Safeguards Rule, the SEC has alleged the companies failed to implement policies and procedures related to encrypting customer PII or employing a firewall to protect web servers.[148] It has not yet alleged in an enforcement action that a failure to have written policies and procedures related to vulnerability management and patch management were a violation of the Safeguards Rule.

However, the SEC's Office of Compliance Inspections and Examinations (OCIE) has released several publications that highlight vulnerability management and patch management. In May 2017, following reports of widespread attacks by the malware WannaCry, OCIE released a "risk alert" that, in an examination of seventy-five registered broker-dealers, investment advisors, and investment companies, all broker-dealers and ninety-six percent of investment management firms had a regular process in place to install software patches.[149] However, the risk alert reported that a minority of the inspected entities had a "significant number of critical and high-risk security patches that were missing important updates."[150] In a 2020 report on "Cybersecurity and Resiliency Observations," OCIE reported that inspected organizations used vulnerability scanning to routinely scan systems within the organization and a patch management program to patch software and hardware.[151] OCIE reiterated the importance of patch management and vulnerability management as a way to "enhance cybersecurity

146. Resolution Agreement, *supra* note 130, at 1–2.
147. 17 C.F.R. § 248.30(a) (2005).
148. R.T. Jones Cap. Equities Mgmt., Inc., No. 3-16827 (S.E.C. Sept. 22, 2015).
149. *Cybersecurity: Ransomware Alert*, OFF. COMPLIANCE INSPECTIONS & EXAMINATIONS 1–2 (May 17, 2017), https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf.
150. *Id.* at 2.
151. Off. Compliance Inspections & Examinations, *Cybersecurity and Resiliency Observations*, U.S. SEC. & EXCH. COMM'N 4–5 (Jan. 27, 2020), https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf.

preparedness and operational resiliency" in a July 10, 2020 risk alert.[152] Specifically, the OCIE risk alert stated, "[i]mplementing proactive vulnerability and patch management programs that take into consideration current risks to the technology environment, and that are conducted frequently and consistently across the technology environment."[153]

These SEC publications indicate that the SEC may consider written policies and procedures for vulnerability management and patch management to be a part of an information security program that is "reasonably designed" to protect customer records and information and in compliance with the Safeguards Rule.

B. State Statutes

Regulators and plaintiffs in private litigation have alleged poor patch management and vulnerability management practices violate certain state statutes. All fifty states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws. In addition to breach notification, half of the states have enacted laws that require certain data security practices. The enforcement mechanism for these laws vary and include private rights of action or enforcement by state regulators. California was the first state to enact both a data breach notification law and a data security practices law. Enacted in 2004, the California data security practices law requires businesses that own or license information about California residents to "implement and maintain reasonable security procedures and practices . . . to protect the personal information . . . ."[154] The law provides a private right of action by an injured party.[155] Many other states have since joined California in requiring reasonable information security. Regulators take the view, as expressed in statements implementing regulations, that these reasonable security practices include patching outdated software.

In a 2016 report, the California Attorney General identified the Center for Internet Security's Critical Security Controls as the minimum level of information security that organizations must meet to have reasonable security.[156] As explained in Section II, CIS Control 3 requires vulnerability management and patch management. In

152. *Cybersecurity: Ransomware Alert*, OFF. COMPLIANCE INSPECTIONS & EXAMINATIONS 2 (July 10, 2020), https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.
153. *Id.* at 3.
154. CAL. CIV. CODE § 1798.81.5(b).
155. CAL. CIV. CODE § 1798.84(b).
156. HARRIS, *supra* note 67, at 30.

the "Message from the Attorney General," then-Attorney General Kamala Harris specifically cited that for the breaches from 2012 to 2015 in California, "nearly all of the exploited vulnerabilities, which enabled these breaches, were compromised more than a year after the solution to patch the vulnerability was publicly available."[157]

Like California, Oregon requires businesses "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information . . . ."[158] The Oregon law also provides examples of reasonable safeguards for companies to use, including "[a]pplying security updates and a reasonable security patch management program to software that might reasonably be at risk of or vulnerable to a breach of security."[159] Massachusetts has a similar requirement in the regulations implementing its data security practices law. Under the regulation, businesses that have systems connected to the internet and containing personal information must have "reasonably up-to-date firewall protection and operating system security patches."[160]

Recently, New York has joined the group of states that requires data security practices. Beginning in March 2020, New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act went into effect. The new law imposes a variety of new information security requirements on companies, including requiring businesses that own or license New York residents' private information "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information . . . ."[161] The law identifies examples of safeguards for companies to adopt to comply with the reasonable security requirement. Included within these safeguards are identifying reasonably foreseeable internal and external risks, assessing risks in network and software design, and regularly testing and monitoring the effectiveness of key controls, systems, and procedures.

C. Common Law Causes of Action

When an attacker successfully breaches a company network and acquires (or in very few states, accesses) PII, state laws may require the company to notify the individuals whose PII has been impacted in certain circumstances. Following the notifications, impacted individuals often file class action lawsuits against the company. The

157. *Id.* at ii.
158. OR. REV. STAT. § 646A.622(1).
159. *Id.* § 646A.622(2)(d)(B)(ii).
160. 201 MASS. CODE REGS. 17.04(6).
161. N.Y. GEN. BUS. LAW § 899-bb(2).

alleged causes of action are varied and can include negligence, negligence per se, gross negligence, and unjust enrichment. Issues related to vulnerability and patch management are emerging as relevant bases for these causes of action.

1. Negligence

In data breach cases, plaintiffs frequently, and often unsuccessfully, allege negligence under a common law tort theory. A claim of negligence requires that a plaintiff allege four elements: duty, breach, causation, and damages.[162] The availability of plaintiffs to successfully allege negligence as a cause of action following a data breach is a contested legal issue. In several jurisdictions, courts have ruled in favor of defendants and have dismissed negligence claims in this context for a variety of reasons.[163] In states where negligence has been an available cause of action in this context, plaintiffs may attempt to allege that a defendant's patch management and vulnerability management procedures are relevant to determining whether the defendant satisfied its duty to use reasonable care to safeguard sensitive personal information. While duty is a question of law, standard of care is a question of fact, established through expert opinion,[164] legislation, regulation, or fixed by the factfinder by applying the facts of the case.[165]

In this context, courts typically have not specified the standard of care required by a defendant, including whether that standard of care requires adequate vulnerability management and patch management. Some courts have referred to the standard in vague

---

162. A general rule of negligence is that "anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act." RESTATEMENT (SECOND) OF TORTS § 302 cmt. a (AM. L. INST. 1965).

163. On a variety of different bases, courts have dismissed data breach cases that allege negligence. *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 977 (N.D. Cal. 2016) (dismissing claims brought under Indiana law for negligence because Indiana law does not provide for a private cause of action for a database owner that fails to adequately protection personal information); *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 477 (D. Md. 2020) (dismissing claims brought under Illinois law for negligence because there is no duty under Illinois law to protect personal information); *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (dismissing claims under Alaska, California, Illinois, Iowa, and Massachusetts law due to the economic loss rule).

164. In medical malpractice cases, determining standard of care "requires expert testimony and presents a question of fact for the jury." K.H. *ex rel.* H.S. v. Kumar, 122 A.3d 1080, 1097 (Pa. Super. Ct. 2015).

165. *See* RESTATEMENT (SECOND) OF TORTS § 285 (AM. L. INST. 1965); *see also* Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) (explaining that while duty is a legal question, the scope of the duty is a question of foreseeability).

"reasonableness" terms.[166] Others have provided more specific references to whether the company used industry standards,[167] whether the company followed its own written policies,[168] and whether the company was aware of the vulnerability that led to the breach.[169] These three characteristics may be relevant in a case where the plaintiffs allege that a defendant failed to patch a known software vulnerability.

a. Cases Referencing Industry Standards

In the privacy class action filed against Target following the cyberattack that affected more than forty-one-million customer payment card accounts, the plaintiffs claimed Target failed to comply with PCI-DSS.[170] The plaintiffs also claimed Target owed a duty "to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting [Plaintiffs'] personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons."[171] Target did not dispute this element, and some of the negligence claims alleging a failure to comply with PCI-DSS survived Target's motion to dismiss. Similarly, the plaintiffs in *Sackin v. TransPerfect Global, Inc.*

166. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1170 (noting that plaintiffs claimed defendants owed a duty "to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting [Plaintiffs'] personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons") (alteration in original); *see also* Hapka v. Carecentrix, Inc., No. 16-2372-CM, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016) (explaining that plaintiffs sufficiently alleged that employer defendants breached their duty to implement reasonable data security measures in "obtaining, securing, safeguarding, deleting and protecting" plaintiffs' personal information from disclosure).

167. *Sackin*, 278 F. Supp. 3d at 744 ("TransPerfect's cyber-security was not up to industry par . . . ."); Wines, Vines & Corks, LLC v. First Nat'l of Neb., Inc., No. 8:14CV82, 2014 WL 12665802, at *5 (D. Neb. Aug. 20, 2014) (holding that plaintiffs' claim that defendants failed to use "reasonable care and conform to industry standards in securing and protect[ing]" plaintiff's account information survived a motion to dismiss).

168. Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (granting defendant's motion for summary judgment in part because defendant followed its own information security policies).

169. Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *13 (D. Mass. Dec. 31, 2019) ("Because Plaintiffs claim that Defendants failed to employ reasonable security measures, including encryption, which was recommended by the Information Technology Department after two previous data breaches and to adequately train its employees to guard against a phishing scam, the Complaint adequately alleges that Defendants breached their duty of reasonable care."); *see also* Bohannan v. Innovak Int'l, Inc., 318 F.R.D. 525, 527 (M.D. Ala. 2016).

170. Amended Complaint at 121, *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1170 (D. Minn. 2014) (No. 14-2522). Notably, PCI-DSS standards require that companies maintain a vulnerability management program. *See infra* Part III.C.

171. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1170 (alteration in original).

alleged that because TransPerfect's cybersecurity was "not up to industry par," an employee responded to a phishing email and sent copies of W-2 forms and payroll information for all current and former employees to a cybercriminal.[172] The court found that plaintiffs sufficiently alleged "TransPerfect violated its duty to take reasonable steps to protect its employees' PII."[173] Specifically, TransPerfect's cybersecurity was "not up to industry par" because it failed to erect a digital firewall, conduct data security training, or adopt retention and destruction policies.[174] The accepted reliance on industry standards indicates that the industry standards set forth in Section II relating to vulnerability and patch management may be considered in determining the duty of care.

b. Cases Referencing Internal Policies

Courts have found that plaintiffs have sufficiently alleged a breach of duty of reasonable care when plaintiffs have alleged that defendants failed to comply with their own policies.[175] In 2015, a trial court in New York concluded that following a breach of health information, the plaintiffs sufficiently stated a negligence claim because the hospital's privacy policy assured the plaintiffs that the hospital would protect the plaintiffs' information and would not disclose it without consent.[176] Conversely, courts have held that defendants acted reasonably when defendants implemented written information security policies.[177] As such, when companies have internal policies relating to vulnerability and patch management, a failure to comply with those policies may also provide a basis for a plaintiff to allege a duty of care existed.

---

172. Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 744 (S.D.N.Y. 2017).

173. *Id.* at 748.

174. *Id.* at 744, 748.

175. Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *13 (D. Mass. Dec. 31, 2019) ("Because Plaintiffs claim that Defendants failed to employ reasonable security measures, including encryption, which was recommended by the Information Technology Department after two previous data breaches and to adequately train its employees to guard against a phishing scam, the Complaint adequately alleges that Defendants breached their duty of reasonable care."); Abdale v. N. Shore Long Island Jewish Health Sys., Inc., 19 N.Y.S.3d 850, 861 (N.Y. Sup. Ct. 2015) (finding plaintiffs' negligence claim survived a motion to dismiss, the court did not analyze the standard of care and noted defendants allegedly informed plaintiffs their personal information would not be shared with third parties absent consent).

176. *Abdale*, 19 N.Y.S.3d at 861.

177. Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (granting defendant's motion for summary judgment in part because defendant followed its own information security policies).

c. Cases Referencing Knowledge

In 2016, Innovak, a creator of administrative software for school districts, announced users' PII had been comprised in a data breach when hackers infiltrated the internet portal where end users accessed their tax and payroll information.[178] In the privacy class action litigation that followed, the plaintiffs claimed that Innovak knew of the vulnerability since 2014 and "failed to take reasonable steps to prevent a breach."[179] Though neither the court nor the plaintiffs articulated a standard of care, Innovak's alleged awareness of its vulnerabilities and its failure to take affirmative steps led the court to deny Innovak's motion to dismiss.[180]

Although the ability for a plaintiff to allege negligence following a data breach is an undecided issue of law, to reduce the legal risk of a cause of action for negligence, these considerations weigh in favor of a company maintaining and implementing an adequate vulnerability management and patch management program, which includes following the written procedures that apply to the program and staying abreast of industry standards.

2. Negligence Per Se

In the context of data breach litigation, plaintiffs have similarly attempted, with mixed results, to use Section 5 of the FTCA and the failure to use "reasonable measures" to protect personal information as the basis for a claim of negligence per se.[181] In states where courts have held that negligence per se applies, plaintiffs have sought to establish a duty through FTC publications and orders related to vulnerability and patch management.

In 2019, an attack on Capital One affected over 100 million consumers in the United States.[182] The plaintiffs alleged that hackers accessed their data by exploiting a "well-known" vulnerability of the Amazon Web Services cloud where Capital One stored consumers' confidential PII.[183] The court found that the plaintiffs plausibly

178. Bohannan v. Innovak Int'l, Inc., 318 F.R.D. 525, 527 (M.D. Ala. 2016).
179. *Id.* at 530.
180. *Id.*
181. *See In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., No. 19-md-2879, 2020 WL 6290670, at *21 (D. Md. Oct. 27, 2020) (dismissing negligence per se claims brought under Maryland law but denying defendant's motion to dismiss negligence per se claims brought under Connecticut and Georgia law); *In re* Capital One Consumer Data Sec. Breach Litig., No. 1:19md2915 (AJT/JFA), 2020 WL 5629790, at *18 (E.D. Va. Sept. 18, 2020) (dismissing negligence per se claims brought under Virginia law but denying defendant's motion to dismiss negligence per se claims brought under New York law).
182. *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 5629790, at *1.
183. *Id.*

alleged a negligence per se claim under New York law, because the plaintiffs plausibly alleged that the FTCA created an enforceable duty in the data breach context and the plaintiffs were of the class the statute was meant to protect—those whose information was allegedly compromised by a data breach.[184] Further, the plaintiffs imported the standard of care from the FTCA, which, as stated earlier, included provisions related to vulnerability and patch management.[185]

Marriott announced in 2018 that hackers had infiltrated its guest reservation database and had been extricating customers' PII for four years.[186] Plaintiffs sufficiently pled negligence per se predicated on violations of Section 5 of the FTCA under Connecticut law and Georgia law, but not under Maryland law.[187] In its opinion, the court rejected defendants' argument that the "FTC Act cannot serve as the predicate for a negligence claim based on the violation of a statute because it does not 'proscribe a particular standard of care.'"[188] The court explained that several courts had rejected similar arguments by "finding that data breach plaintiffs adequately had pleaded claims of negligence *per se* based on alleged violations of Section 5 of the FTC [A]ct."[189] Because a violation of Section 5 of the FTCA can serve as a predicate for a negligence per se claim, the vulnerability management and patch management considerations within that Act may be considered as part of the risk of civil liability in a class action.

V. CONCLUSION

Though adequate cybersecurity is in many ways viewed as a subjective metric that can be based on factors specific to a company's size, industry, and risk profile, objective measures applicable to general categories of security functions continue to come into focus. Developing caselaw and language relating to regulatory enforcement are making it apparent that vulnerability and patch management are widely becoming recognized as essential functions of an adequate cybersecurity program. Thus, vulnerability and patch

184. *Id.*

185. *Id.* The court found defendants' alleged violations of Section 5 of the FTC did not predicate a negligence per se claim under Virginia law, because only statutes "enacted for public safety" may give rise to negligence per se claims. *Id.* at *18.

186. *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., No. 19-md-2879, 2020 WL 6290670, at *1 (D. Md. Oct. 27, 2020).

187. *Id.* at *24. The court dismissed the negligence per se action under Maryland law because it does not recognize an independent cause of action. *Id.* at *21.

188. *Id.* at *10.

189. *Id.*

management are no longer purely technical functions which concern only a company's IT department, because their existence and sufficiency within a company's cybersecurity program have likewise become the subject of scrutiny of regulators and plaintiffs alike. As such, legal departments are increasingly having to take notice of their company's vulnerability management and patch management programs and evaluate the potential legal risk they pose to the company, even before a data breach occurs.