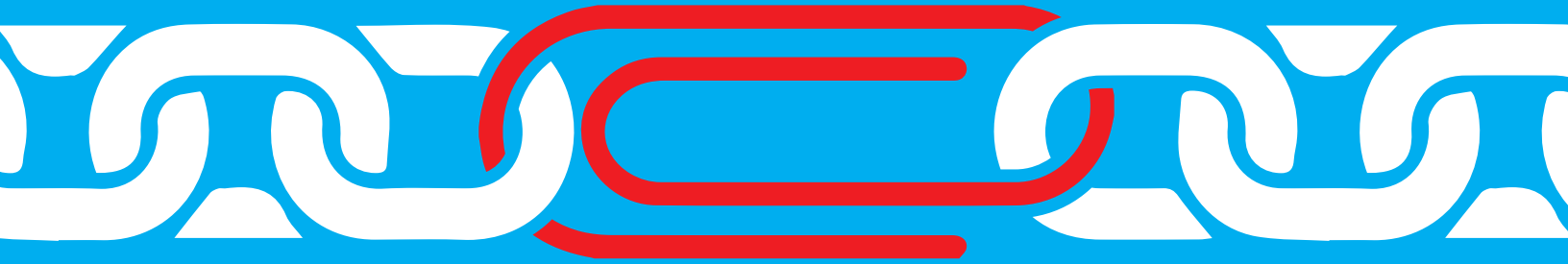


Center for  
Cybersecurity



# THIRD-PARTY CYBER RISK & CORPORATE RESPONSIBILITY

Judith H. Germano



# THIRD-PARTY CYBER RISK & CORPORATE RESPONSIBILITY


Judith H. Germano  
February 2017

Copyright © Center for Cybersecurity 2017

All rights reserved. No part of the publication may be reproduced, stored in a retrieval system, translated, or transmitted in any form or by any means now or hereafter known, electronic or mechanical, without permission in writing from the copyright holder.

New York University School of Law  
139 MacDougal Street  
New York, NY 10012  
212.992.8854

[ccs@nyu.edu](mailto:ccs@nyu.edu)  
[cyber.nyu.edu](http://cyber.nyu.edu)



*Third parties, including law firms, accounting and marketing firms, technology providers, subcontractors, janitors and others who provide a wide range of professional, administrative, supply-chain and other services, are a significant source of cybersecurity vulnerabilities; yet there remains much work to be done in terms of how third-party risk is assessed and controlled. Executives, board members and their strategic and legal advisors, as well as government regulators and lawmakers, need to understand better: (1) How to identify and assess third-party cyber risk; (2) What regulatory and civil liability concerns exist regarding third-party cyber risk; and (3) What corporate governance framework and operational solutions most effectively address that risk. Properly understanding and addressing third-party cyber risk requires a proactive and comprehensive approach to enable parties on all sides to prevent harms and to prepare for and respond to incidents in a faster, better coordinated, less expensive and more effective manner.*

John Donne did not have a computer, but he did have a point: “No [person] is an island...” This is particularly true when it comes to network security. Contemplating multiple access points to a corporate network, and to sensitive company data and personal information that resides within and outside that network, may be enough to keep informed corporate officers and directors awake at night. Indeed, the catalogue of security risks that might impact that data appears to be unlimited. Third parties, including law firms, accounting and marketing firms, technology providers, subcontractors, janitors and others who provide a wide range of professional, administrative, maintenance and supply-chain services, are significant sources of cyber risk. Large institutions may have thousands, and sometimes tens of thousands, of vendors.<sup>1</sup> Indeed, there is a seemingly endless list of affiliates, agents, partners, customers, clients, correspondent banks, and others who provide an essential role in an enterprise’s life yet also increase risk.

There remains much work to be done in terms of how third-party risk is assessed, regulated and controlled. Despite spending hundreds of millions of dollars on security, companies remain vulnerable to losing critical, sensitive information via a broad range of third parties with access to that information, and to the companies’ systems. It is not always clear what measures are necessary and available for companies of varying sizes and budgets to assess and mitigate that risk, and the law continues to evolve regarding how that risk is allocated in the regulatory and civil liability context.

The challenge of third-party risk is significant, yet the strategic solutions from a legal, governance and technological perspective remain insufficiently developed. Executives, board members and their strategic and legal advisors, as well as government regulators and lawmakers, need to better understand: (1) How to identify and assess third-party cyber risk from a governance and operational perspective; (2) What regulatory and liability concerns exist regarding third-party cyber risk; and (3) What corporate

governance framework and operational solutions most effectively address that risk.

## 1. Assessing Third-party Cyber Risk

Protecting an enterprise’s proprietary information and systems is a major challenge, made all the more complex by the significant vulnerabilities created by third parties with access to non-public company information and systems. As large enterprises become more sophisticated and effective at cybersecurity, criminals increasingly will identify the path of least resistance, seeking out alternative means for infiltrating systems and obtaining data, including through third-party providers.

### THIRD-PARTY RISK IS SIGNIFICANT

The headlines are replete with examples of third-party breaches, including vendors mishandling data, compromised credit card payment processors and other, multiple access points of vulnerability. Listing the “Top Financial Services Cyber Security Trends for 2015,” the firm Booz Allen Hamilton put third-party risk at the top of the list of concerns, recognizing that in financial services, like in many sectors, there is a “huge mesh of intertwined capabilities.”<sup>2</sup> Vast capabilities and connections create additional portals of vulnerability that must be managed. We are all too familiar with the fact that credit card and personal data of more than 110 million customers of Target Corp. was exposed after hackers gained access via Target’s HVAC vendor. Information regarding Target’s vendors was available via a simple Google search revealing Target’s Supplier Portal.<sup>3</sup> The hackers then sent a phishing email laced with the widely used Citadel password-stealing malware (a derivative of the Zeus banking trojan), which is a massively distributed bot that has compromised millions of computers, to Target’s HVAC supplier. When an employee at the Pennsylvania-based heating, air conditioning and refrigeration company was duped by the phishing email, Citadel malware enabled hackers to steal employee credentials that ultimately

<sup>1</sup> Arjun Sethi & Uday Singh, “Managing Vendors Involves Managing Risk,” Am. Banker, April 4, 2013, available at <http://www.americanbanker.com/bankthink/managing-vendors-involves-managing-risk-1058018-1.html> (“Most large institutions have over 1,000 vendors, many have tens of thousands.”).

<sup>2</sup> Press Release, Booz Allen Hamilton, “Booz Allen Releases Annual Financial Services Cyber Trends for 2015,” (Nov. 19, 2014), available at <http://www.boozallen.com/media-center/press-releases/2014/11/booz-allen-releases-annual-financial-services-cyber-trends-for-2>.

<sup>3</sup> Brian Krebs, “Email Attack on Vendor Set Up Breach at Target,” KrebsonSecurity (Feb. 14, 2014), <http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/>.

were used to access Target's systems as a portal for the massive breach.<sup>4</sup>

Another example of the significance and scope of third-party risk is an international hacking and securities fraud scheme, involving confidential corporate information siphoned from newswires entrusted with that information prior to its public disclosure.<sup>5</sup> The criminal indictments, brought by U.S. Attorney's Offices in the District of New Jersey and the Eastern District of New York, and the related civil complaint by the U.S. Securities and Exchange Commission, alleged that a band of a sophisticated, international criminals compromised the networks of three major newswire companies, Marketwire, Business Wire and PR Newswire, and stole more than 150,000 yet-to-be published press releases from a number of companies. Those press releases contained material, nonpublic information regarding the companies' earnings, gross margins and revenues, as well as other confidential information. The hackers then funneled that information to traders who bought and sold stock based on the information that was soon to be released. According to the government, and the guilty pleas of one charged hacker and two traders in the case, the conspirators made more than \$30 million in illegal trading profits.<sup>6</sup> Confidential valuable company information of numerous companies, including Panera Bread, Boeing, Hewlett-Packard and Oracle, among many others, was compromised through this third-party security attack.<sup>7</sup>

As the newswire securities-hacking case illustrates, often, it may not be the enterprise that is actually breached but rather its clients or partners, even though negative news about a data breach (which

many consumers and shareholders often remember best) tends to focus on the company whose data is leaked rather than the precise vector of attack. The public breaches of Snapchat and Dropbox were the result of an actually exploited vulnerability in the third-party app, SnapSave. To note several other examples of third-party breaches:

- T-Mobile had records of 15 million customers exposed (including Social Security numbers, birthdays, driver license/passport numbers and more) due to a server breach at Experian, the company T-Mobile used for customer credit assessments.<sup>8</sup>
- Lowe's suffered from a vendor error when its cloud provider hired to store sensitive personal identification information of certain current and former employees unintentionally backed up the data to an insecure computer server accessible from the Internet.<sup>9</sup>
- Home Depot had payment card information of more than 50 million customers exposed after hackers used credentials stolen from a third-party vendor to access Home Depot's systems and insert malware on self-checkout systems. Home Depot offered \$19.5 million to settle related class action lawsuits.<sup>10</sup>
- Walmart, Costco, CVS, Rite-Aid, Sam's Club and Tesco had their photo centers compromised, exposing customers' credit card and personal data, when PNI Digital Media, a Staples subsidiary that hosts the photo centers, was breached.<sup>11</sup>
- RT Jones Capital, a regulated investment advisor, was exposed to SEC charges when a third-party hosted web server was breached, compromising personal information of approximately 100,000 individuals and thousands of the firm's clients.<sup>12</sup>

<sup>4</sup> *Id.*

<sup>5</sup> Press Release, Fed. Bureau of Investigation, "Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme," (Aug. 11, 2015), available at <https://www.fbi.gov/newyork/press-releases/2015/nine-people-charged-in-largest-known-computer-hacking-and-securities-fraud-scheme>.

<sup>6</sup> See, e.g., U.S. Dept. of Justice Press Release, "Ukrainian Hacker Admits Role in Largest Known Computer Hacking and Securities Fraud Scheme," May 16, 2016, available at <https://www.justice.gov/usao-nj/pr/ukrainian-hacker-admits-role-largest-known-computer-hacking-and-securities-fraud-scheme>.

<sup>7</sup> *Id.*

<sup>8</sup> T-Mobile website, Frequently Asked Questions About the Experian Incident, Sept. 2015, <http://www.t-mobile.com/landing/experian-data-breach-faq.html>.

<sup>9</sup> Steve Ragan, "Vendor Error Forces Lowe's to Issue Breach Notification Letters," CSO (May 22, 2014), <http://www.csoonline.com/article/2158122/identity-management/vendor-error-forces-lowes-to-issue-breach-notification-letters.html>.

<sup>10</sup> Steven Musil, CNET, "Home Depot Offers \$19 Million to Settle Customer Hacking Lawsuit," March 8, 2016, available at <https://www.cnet.com/news/home-depot-offers-19m-to-settle-customers-hacking-lawsuit/>.

<sup>11</sup> Doug Olenick, "Customer Data Possibly Compromised in Online Photo Store Malware Attack," SCMag. (Sep. 14, 2015), <http://www.scmagazine.com/pni-digital-media-cvs-and-costco-warn-of-pii-compromise-in-photo-center-attack/article/438472/>.

<sup>12</sup> Press Release, SEC, "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach," (Sep. 22, 2015), available at <https://www.sec.gov/news/pressrelease/2015-202.html>.

- GMR Transcription Services faced an FTC complaint when contractors uploaded highly sensitive medical data of GMR's corporate customers in a way that made it publicly available via an internet search engine.<sup>13</sup>
- Goodwill Industries International, a retailer, had customer credit card data stolen via inadequate security at one of its payment processors.<sup>14</sup>
- Boston Medical Center experienced a healthcare data breach when a third-party transcription service posted, without adequate password and encryption protection, doctors' notes of 15,000 patients (including what medications they were taking), making that information publicly accessible online.<sup>15</sup>
- J.P. Morgan Chase outsourced management of its Corporate Challenge Race registration to a firm in Michigan, which was hacked. In an interesting turn, that third-party breach led J.P. Morgan Chase to discover the same perpetrators also had infiltrated the bank itself, albeit via a different means of access.<sup>16</sup>
- Epsilon Data Management, which managed emails for many large companies, exposed more than 60 million records of clients including Best Buy, Chase, Kroger, JP Morgan, Target, TiVo and Walgreens.<sup>17</sup>

These and other examples illustrate the multifaceted challenges to understanding and managing third-party cyber risk. Unfortunately, many solutions remain in the nascent stages and it is essential that companies think proactively about third-party risk governance across the enterprise.

### THIRD-PARTY RISK GOVERNANCE

Often, companies rely on outsourcing either to access necessary expertise, or as a less expensive alternative to handling professional, technological, maintenance

and other services in-house. The third-party nature of the relationship creates difficulty and an inherent reluctance to spending additional resources securing, or at least overseeing, the systems of those third parties. In the first instance, it can be challenging to conduct the due diligence required to determine whether a third party's security practices pose an unacceptable risk to an organization. These challenges include, for example, getting an organization to focus on technical security as an important matter, and finding the right people on both sides of the discussion who can, and are authorized to, identify, request, provide and verify the necessary information in a meaningful and efficient way. The problem is made more challenging due to a lack of standard security practices for evaluating particular scenarios, as well as difficulties in verifying that the information is, and continues to be, accurate during the course of the third-party relationship. Yet investing the human and financial capital proactively to assess and mitigate third-party risk can help significantly reduce costs associated with a potential breach derived from a business relationship with a third party.

Major challenges to assessing third-party risk are both of a governance and operational nature. Corporate decision makers need to balance speed, innovation and efficiency with security, and make informed decisions regarding who has what level of access to what portions of the enterprise's systems or sensitive data.

In terms of effective governance, too many companies are still struggling to address their own internal network security issues and have not sufficiently considered the risks to their confidential information from vulnerabilities that lurk beyond their own networks. But third-party risk (as well as internal network security) is too significant and potentially

<sup>13</sup> Press Release, FTC, "FTC Approves Final Order in Case Against GMR Transcription Services," (Aug. 21, 2014), available at <https://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services>.

<sup>14</sup> Kate Vinton, "868,000 Payment Cards, 330 Stores Hit in Goodwill Credit Card Breach," FORBES (Sep. 3, 2014), <http://www.forbes.com/sites/katevinton/2014/09/03/868000-payment-cards-330-stores-hit-in-goodwill-credit-card-breach/#27bdcf2a1878>.

<sup>15</sup> Robert Weisman, "Boston Medical Center Fires Vendor After Data Breach," BOS. GLOBE (Apr. 29, 2014), <https://www.bostonglobe.com/business/2014/04/29/boston-medical-center-fires-vendor-after-data-breach/jboHN1Aq1x2JAE5amyEHI0/story.html>; Sara Health, "Boston Medical Center May Face Healthcare Data Breach Lawsuit," HEALTH IT SEC. (Jan. 6, 2016), <http://healthitsecurity.com/news/boston-medical-center-may-face-healthcare-data-breach-lawsuit>.

<sup>16</sup> Danny Yadron & Emily Glazer, "J.P. Morgan Found Hackers Through Breach of Road-Race Website," WALL ST. J. (Oct. 21, 2014), <http://www.wsj.com/articles/j-p-morgan-found-hackers-after-finding-breach-of-race-website-1414766443>; Matthew Goldstein, *4 Arrested in Schemes Said to Be Tied to JPMorgan Chase Breach*, CNBC (July 22, 2015), <http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html>.

<sup>17</sup> Darlene Storm, "Epsilon Breach: Hack of the Century?," COMPUTERWORLD (Apr. 4, 2011), <http://www.computerworld.com/article/2471044/cloud-computing/epsilon-breach-hack-of-the-century-.html>; Ben Worthen, "Breach Brings Scrutiny," WALL ST. J. (Apr. 5, 2011), <http://www.wsj.com/articles/SB10001424052748704587004576245131531712342>.



too dangerous an issue for corporate executives and board members to continue to overlook. Indeed, recent cases seeking to hold board members and executives accountable for network breaches, including, for example, at Target, Wyndham and Home Depot, make clear that it is no longer acceptable to hold one's breath and hope it is not his or her company's turn in the data breach headlines.<sup>18</sup>

Companies must develop an effective risk management framework that identifies the key information and operations they seek to protect, and examine where and how that data resides and travels, or can be accessed, from inside and also beyond the company's networks. While this task may seem an overwhelming analysis of an eternal parade of horrors – thereby causing many busy executives to shun the topic – the current risk and liability landscape shows that it is a necessity. Effective cyber risk governance requires corporate executives to become sufficiently informed of risks within and beyond their own networks and then make considered judgments about areas where it is appropriate to take on risk, and how to price and mitigate unavoidable risks from cyber harms, as businesses do with other parts of their operations. There are instances when a company cannot provide sufficient security for managing particular information or business functions and outsourcing to cloud providers or other third parties with higher levels of security may be the safer decision. Other times, the data or function is better maintained internally provided it is properly secured. Either way, it is essential that the company make informed and thoughtful decisions regarding what information it has, how it is being protected and who may have access to the information and systems.

#### OPERATIONALIZING THE SOLUTION

To tackle the challenge of third-party cyber risk from an operational standpoint, an essential first step is to understand its multi-faceted and widely distributed nature throughout the enterprise. For many companies, the organizational (and attendant) risks may be sprawling, making it essential to prioritize security

solutions that focus on the information and access points that the company deems most valuable to protect. It also is important to have one person, or a small group of people, specifically tasked with managing these issues, both in identifying and valuing data and ensuring it is sufficiently protected from vulnerabilities within and outside the organization. As a basic starting point in dealing with third parties, the company should be careful to allow third parties to access only the information and network entry points that are necessary to perform their current assignments. Companies also should put in place systems to:

- Verify that third-party providers are knowledgeable, and also trustworthy, regarding their stated security measures;
- Ensure those at the company who are working with third parties not only ask the right questions but also provide the necessary follow-up to the answers received before providing access to data or systems;
- Establish meaningful audit procedures and consequences for violating audit requirements that are written into contracts with vendors from the negotiation stage;
- Ensure that the right people within an organization, who are capable of identifying and addressing security concerns, are involved in the procurement process;
- Establish the procedures for escalation and decision-making that are necessary for balancing tradeoffs that may become apparent in the course of discussions with third-party providers;
- Properly terminate third-party relationships, and retrieve or cut off access to data as appropriate; and
- Evaluate how to transfer risk and liability, as appropriate, through contracts and insurance.

Despite these measures, however, it also is essential that members of senior leadership understand that, even with third-party safeguards, the ultimate burden – measured primarily by customer trust and confidence, public reputation, and potential regulatory and private civil liability – may not easily be transferrable (if at all). Thus, it is essential to have a plan in place for

<sup>18</sup> See, e.g., *In re Target Corp. Data Sec. Breach Litigation*, 66 F. Supp. 3d 1154 (D. Minn. 2014); *Palkon v. Holmes*, No. 2:14-CV-01234, 2014 WL 5341880 (D. N.J. Oct. 20, 2014); *Complaint, Bennet v. Home Depot*, No. 1:15-CV-02999 (N.D. Ga. Sep. 2, 2015); *In re Heartland Payment Systems Security Litigation*, No. 09-1043, 2009 WL 4798148, (D. N.J. Dec. 7, 2009).

responding to breaches not only of the organization, but also specifically as a result of third-party vulnerabilities. It also is essential that the company provides meaningful processes for managing the relationships and risks associated with third parties, and ensuring there is sufficient oversight and review of those relationships and risks.

There has been progress in improving metrics for assessing risk and ensuring effective controls but more needs to be done. It is critical that companies consider not only their own systems but also external risks that may expose those systems, and implement ways to identify and measure that risk. This starts first with identifying sensitive information and determining where, internally and also externally, that information resides and how it can be accessed. While a deceptively simple first step, determining with some degree of certainty where sensitive information resides and how it can be accessed in a large global corporation can be a challenge in itself. Such a challenge is magnified over time, as a company grows and adds businesses, technologies and resources. Second, it requires understanding the security of that information and imposing controls commensurate with the sensitivity of the data. And third, the security controls need to be reviewed and assessed with some regularity, either by the enterprise or by a certification or review process conducted by (yet another) third party.

To properly tackle each of these challenges, companies need to approach cyber risk in a thoughtful and right-sized manner. Yet many companies have not yet passed this first stage of determining what data and entities are factors to be managed. The November 2013 PwC Global State of Information Security Report noted that 69% of companies surveyed lack an adequate record of all places their data is stored, and 74% do not keep a complete inventory of all third-party suppliers that handle employee and customer data.<sup>19</sup> Two years later, in the 2015 PwC U.S. State of Cybercrime Survey, only 42% of companies surveyed consider supplier risks, 23% said they do not evalu-

ate third parties at all, and the report stated that most companies lack a process for assessing security of third-party partners.<sup>20</sup>

Properly managing third-party cyber risk must be an active concern, and it requires an active response for managing, mitigating and monitoring that risk. No longer is it sufficient to have vendors self-certify that they are secure; reasonable but in-depth review and oversight is required when it comes to handling sensitive data and accessing systems. Determining what that ongoing review entails is a significant challenge for company management.

## 2. Third-party Regulatory and Civil Liability Concerns

As systems become increasingly complex, and companies or their employees rely increasingly on cloud computing, mobility, apps and external technical service providers, the network of risk becomes even more threatening. This might encourage companies to turn away from outsourcing where possible and keep more work and information in-house. Yet that creates problems in terms of capacity and feasibility, limiting expertise while potentially increasing cost, and also – significantly – may result in increased liability risk.

A major factor in addressing third-party risk is understanding who bears the burden of providing security and evaluating, on behalf of one's own enterprise, whether that burden can or should be shifted to someone else. A company may not want to outsource if it can provide the same services internally with greater security. But that is not always the case. A company (particularly one with sharply limited resources) that retains all its information processing and security controls internally may lose an opportunity to obtain greater security at a lower cost through outsourcing. By not outsourcing, the company also restricts its potential ability, in the event of a breach, to transfer liability (based on contract or responsi-

<sup>19</sup> PRICEWATERHOUSECOOPERS, PWC VIEWPOINT ON THIRD PARTY RISK MANAGEMENT 5 (Nov. 2013), available at <https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-viewpoint-vendor-risk-management.pdf>.

<sup>20</sup> PRICEWATERHOUSECOOPERS, US CYBERSECURITY: PROGRESS STALLED 12 (July 2015), available at <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf>, page 12.



bility) – and also reputational risk - to a third party. Relying on a trusted and responsible third party may bring the benefit, in the event of a breach, of “standing with the pack,” shifting the focus and reputational damage from the company that outsourced to the third party that was breached. But outsourcing does not absolve a company from oversight duties, or potential liability in the event of a breach, even when the third party is the weak link. Thus, a company without sufficient third-party oversight controls might find itself in the unfortunate position of being held liable for the loss of its information from a third party whose security practices it cannot (by contract or otherwise) control.

In one example, Boston Medical Center (BMC) faced a class-action lawsuit due to a data breach caused by a third-party vendor.<sup>21</sup> BMC used an independent medical records transcription service, MDF Transcription Services, to transcribe doctors’ notes, including regarding health conditions and medications of 15,000 patients. The service then posted those notes to its online site without adequate password and encryption protection, thereby making the notes publicly accessible. BMC had used MDF Transcription Services for 10 years. On the day BMC learned (via an outside service provider) that the records were exposed, it immediately contacted MDF, the website was removed from the Internet that day and BMC promptly notified those who potentially were impacted by the exposure.<sup>22</sup> Although the plaintiff-patients did not allege in the complaint that the records were actually accessed or that any unauthorized person used their personal information, a Massachusetts Superior Court judge nonetheless denied BMC’s motion to dismiss the case for lack of standing.<sup>23</sup> This case casts a spotlight on the degree of oversight and monitoring BMC had over its long-standing vendor, and steps that BMC took, or failed to take, to ensure that patient medical information

was adequately protected not only by BMC but also by BMC’s third-party vendor throughout the process.

Current regulatory initiatives are increasingly requiring companies and institutions to take responsibility for ensuring, to some degree, that third-party vendors and other providers are sufficiently secure. On September 13, 2016, the New York Department of Financial Services (DFS) proposed requirements that banks and insurers adopt written cybersecurity policies and designate Chief Information Security Officers; with regard to third-party providers, the proposed regulations require multifactor authentication, data encryption, loss indemnification, warranties, incident notices and audits.<sup>24</sup> In response to push-back it received from commentators and financial industry groups,<sup>25</sup> DFS announced a revised version of these proposed regulations on December 28, 2016, and extended the comment period to March 2017; the updated proposal still requires a “Third-Party Service Provider Security Policy” (Section 500.11), but one that is now more risk-based than the original version.<sup>26</sup> Other announcements, bulletins and letters have issued from the U.S. Treasury, U.S. Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), the National Institute for Standards and Technology (NIST) and elsewhere.<sup>27</sup> These regulatory interventions have encouraged, and in some cases required, a level of due diligence and reporting on a range of third-party risk issues, including: planning; due diligence; contract negotiation; ongoing monitoring; oversight and accountability; relationship termination; documentation and reporting; independent reviews; supervisory review of third-party service providers; and other measures.<sup>28</sup>

With this obligation of due diligence comes a greater risk of regulatory and civil liability if and when those obligations are not met. Regulatory agencies, includ-

<sup>21</sup> *Walker v. Boston Med. Ctr Corp.*, 33 Mass. L. Rptr. 179 (Mass. Super. Ct. Nov. 20, 2015); Sara Health, *Boston Medical Center May Face Healthcare Data Breach Lawsuit*, HEALTH IT SEC. (Jan. 6, 2016), <http://healthitsecurity.com/news/boston-medical-center-may-face-healthcare-data-breach-lawsuit>.

<sup>22</sup> Robert Weisman, *Boston Medical Center Fires Vendor After Data Breach*, BOS. GLOBE (Apr. 29, 2014); <http://www.bostonglobe.com/business/2014/04/29/boston-medical-center-fires-vendor-after-data-breach/jboHN1Aq1x2JAE5amyEHIO/story.html>.

<sup>23</sup> *Walker*, 33 Mass. L. Rptr. 179.

<sup>24</sup> NY DFS, Press Release, “Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and financial Institutions,” Sept. 13, 2015.

<sup>25</sup> Proposed 23 NYCRR 500, Rev. Dec. 28, 2016, available at <http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf>.

<sup>26</sup> The author’s comments regarding the initial version of the proposed regulations can be found at: Judith Germano, FORBES, “Proposed NY Cybersecurity Regulation: A Giant Leap Backward?” Dec. 2, 2016, available at <http://www.forbes.com/sites/realspin/2016/12/02/proposed-ny-cybersecurity-regulation-a-giant-leap-backward/#619bbc522e78>.

<sup>27</sup> See Securities Industry & Financial Markets Association, *Resource Center*, SIFMA, <http://www.sifma.org/issues/operations-and-technology/cybersecurity/third-party-risk-management/> (last visited Mar. 5, 2016) (listing and providing links to 17 different regulatory provisions).

<sup>28</sup> A helpful table of these third-party risk requirements across 17 different regulatory provisions is available at: [http://www.sifma.org/uploadedfiles/issues/technology\\_and\\_operations/cyber\\_security/summary%20third%20party%20regulation%20mapping%20table.pdf?n=10743](http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/summary%20third%20party%20regulation%20mapping%20table.pdf?n=10743)

ing the FTC, SEC and others, increasingly require companies to ensure they are taking sufficient measures to secure sensitive information. To be effective, a company must have written cybersecurity policies, plans and procedures that not only encompass its internal records and operations, but also take into account the security of company data stored with, or managed or accessed by, third parties. Private civil litigants then look to those regulatory enforcement examples as a guidepost when suing companies for failure to meet those standards.<sup>29</sup>

In September 2015, the SEC settled charges against RT Jones Capital Equities Management, an investment advisor located in St. Louis, Missouri, based on a 2013 breach that compromised personal information of approximately 100,000 people, including thousands of the firm's clients. The breach occurred at the third-party hosted web server that stored clients' personally identifiable information. Upon discovering the breach, RT Jones hired at least two consulting firms, traced the attack to China, and provided impacted consumers with notice and free identity theft monitoring. To date, there has been no apparent financial harm to clients as a result of the breach. Yet the SEC issued a cease and desist order, censured RT Jones and required it to pay a \$75,000 fine. The SEC alleged that RT Jones violated the "Safeguards Rule," which requires it to protect consumer records, by failing to establish the requisite, written cybersecurity policies and procedures before the breach.<sup>30</sup> Specifically, RT Jones failed to: conduct periodic risk assessments; implement a firewall; encrypt personally identifiable information stored on its server; and maintain a responsible incident management plan.<sup>31</sup>

In January 2014, the FTC filed a complaint against GMR Transcription Services and its two principal owners, for mishandling, through the use of GMR's

contractors, highly sensitive medical information that GMR was transcribing for medical providers and others. A number of customers – including hospitals, healthcare providers, university students and faculty and "well known corporations" in the retail, insurance, telecom and financial services sectors, as well as government agencies – outsourced their transcription needs to GMR.<sup>32</sup> GMR then hired contractors to transcribe the audio files of records; the contractors downloaded the files, transcribed them and uploaded the transcripts for GMR to then provide to customers. A key problem, however, was that the upload was done in a way that enabled the transcripts to be indexed and made publicly available by a major internet search engine.<sup>33</sup> These records contained highly sensitive information, including regarding medical examinations of children, psychiatric disorders, drug abuse, alcohol use, and pregnancy loss. This case highlights the importance of auditing vendors and service providers to obtain some reasonable degree of insight into the practices of their contractors and vendors. The goal is knowing whether sensitive information will be restricted to specified individuals, or at least to individuals or entities that have been sufficiently vetted or certified, and will be transmitted and handled pursuant to appropriately secure procedures.

In addition to regulators, private civil litigants also seek to hold companies accountable when third parties are the point of vulnerability. Target has paid more than \$116 million in civil settlements related to the 2013 breach that impacted personal information of 110 million customers, with Target's costs, including those settlements, exceeding \$290 million.<sup>34</sup> In December 2014, a federal District Judge in the Target litigation denied Target's motion to dismiss the negligence claim that certain banks that had issued credit cards compromised in the breach brought against Target. The banks alleged that, notwithstanding

<sup>29</sup> JUDITH H. GERMANO & ZACHARY K. GOLDMAN, CTR. ON L. & SEC, AFTER THE BREACH: CYBERSECURITY LIABILITY RISK (2014), available at <http://www.lawandsecurity.org/wp-content/uploads/2014/06/CLS-After-the-Breach-Final.pdf>.

<sup>30</sup> R.T. Jones Equities Capital Mgmt, Inc., No. 3-16827, SEC Admin. Proceeding (2015), available at <https://www.sec.gov/litigation/admin/2015/ia-4204.pdf>. The SEC's press release announcing the RT Jones settlement is available at: (<https://www.sec.gov/news/pressrelease/2015-202.html>).

<sup>31</sup> *Id.*

<sup>32</sup> FTC Complaint, GMR Transcription Services, Inc., No 122-3095 (2014), available at <https://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf>.

<sup>33</sup> Press Release, Federal Trade Commission, Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information, (Jan. 31, 2014), available at <https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it>.

<sup>34</sup> Kevin McGinty, "Target and Card Issuers Reach Final Data Breach Settlement," National Law Review, Dec. 12, 2015, available at <http://www.natlawreview.com/article/target-and-card-issuers-reach-final-data-breach-settlement>.

the fact that the breach was via a third-party HVAC vendor, Target was negligent in failing to provide sufficient security to prevent hackers from accessing customer data and “failed to heed warning signs” that would have stemmed banks’ losses. The banks argued that Target caused and exacerbated the harm and was “solely able and solely responsible” to safeguard the data. The Court found that, even though third-party hackers’ activities caused the harm, the banks sufficiently alleged negligence because “Target played a key role in allowing that harm to occur.” Any relief companies may seek in the specific facts of Target’s actions of purposefully disabling a security feature and failing to heed warnings of intrusion is wisely tempered by the Court’s further statements that (1) its ruling: “will aid Minnesota’s policy of punishing companies that do not secure consumers’ credit- and debit-card information”; and (2) the Court reached that conclusion “despite Target’s dire warnings about the burden of imposing such a duty.”<sup>35</sup> Also, as noted above, Home Depot agreed to pay \$19 million to settle civil claims from a breach that occurred after hackers stole access credentials from a third-party vendor.<sup>36</sup>

These examples send a resounding message that, at least in some jurisdictions, corporate victims will be held accountable even when a third-party vulnerability leads to a breach. Accordingly, not only the reputational and direct damages may be borne by the enterprise, but also a significant degree of regulatory and civil liability risk and responsibility rests with the enterprise, despite vulnerabilities of third-party vendors. This underscores the importance of addressing the issue of third-party risk on an enterprise-wide basis.

### 3. Effective Governance Framework and Solutions

An alarming number of companies either remain unaware of third-party risk, or have not developed coherent systems for managing the risk due to cost or

inconvenience. Companies on both the providing and receiving sides of the relationship need to become more aware of the threat and also become better equipped to tackle and overcome the challenges of managing third-party risk.

This starts with asking what is the right-sized way to address third-party risk for the particular organization, and who (internally and externally) will oversee and guide the management of this process. Cybersecurity is an enterprise risk that requires input from key stakeholders throughout the organization. Third-party contracts should be monitored and centralized, with direction from senior management regarding how security protocols regarding third-party contracts are developed, imposed and monitored, and what tradeoffs are acceptable given the company’s overall risk appetite. Those protocols will vary based on the nature of access a third party may have – third parties accessing more sensitive information should be required to follow more stringent standards and be subject to increased oversight. And the enterprise should be careful only to grant the access necessary for the third party to perform the necessary function.

The interconnected nature of an enterprise with a wide range of third-party providers underscores the substantial differences in how companies handle cybersecurity. There are great variations between the deli that emails daily lunch menus as .jpg files to its customers and the major corporation or financial institution whose employees open those “daily menu” file attachments. In the IT system administration context, the 2013 Trustwave Global Security Report on 450 global data breach investigations noted that 63% were linked to a third party providing technical support, development or maintenance.<sup>37</sup>

Yet, despite this significant vulnerability, often the individuals who understand and are responsible for security are not the ones making decisions regarding procurement and enterprise-wide risk management. This is a significant organizational challenge. To be truly thoughtful and effective in addressing third-

<sup>35</sup> *In re Target Corp. Customer Data Security Breach Litig.*, 64 F.Supp. 3d 1304 (D. Minn. 2014). This case ultimately was settled: see <http://www.nationallawjournal.com/id=1202743809660/Target-Pays-39M-to-Resolve-DataBreach-Litigation?slreturn=20160206213502>.

<sup>36</sup> *Supra*, note 11.

<sup>37</sup> TRUSTWAVE, 2013 GLOBAL SECURITY REPORT 10 (2013), available at <https://www.trustwave.com/Company/Newsroom/News/Trustwave-Reveals-Increase-in-Cyber-Attacks-Targeting-Retailers,-Mobile-Devices-and-E-Commerce/>.

party risk requires an enterprise-wide approach that considers and addresses the concerns of knowledgeable stakeholders across the enterprise.

The cost and burden of cybercrime is distributed among parties to transactions in different ways, depending on the parties' size and sophistication and what is at stake. Often, the larger party in the contractual relationship has the greater bargaining power and therefore can impose its terms on the other, but the desired level of security is not always feasible or appropriate when balanced with expense, complexities and expertise. These issues (when not ignored entirely and to the parties' detriment) often are handled through contract negotiations. Traditionally, in the credit card context, the merchant's bank paid large interchange fees, negotiated through a complex series of contractual agreements between merchants, payment processors and credit card companies. As the Target litigation between the retailer and the banks demonstrates, however, such contracts and long-established practices do not provide complete certainty as to how cyber risk is allocated. The brewing series of civil actions and the substantial increase in regulatory scrutiny is likely to impact how risk is allocated with regard to payment processing in the retail sector. The litigation also may impact contractual relationships between other service providers and in other sectors.

To address these concerns, companies must define security procedures and policies, and consider liability and indemnification provisions that correspond to the value of data at issue. But those agreements need to be sufficiently flexible to account for changing laws, tools and processes; and many older agreements (particularly those that implicate sensitive data or significant system access) may need to be re-addressed. There also need to be right-sized security assessments that identify gaps and vulnerabilities, explore how past incidents were handled and determine how security was improved as a result.

Companies also should include vendors in their own incident response plans, risk assessments and tabletop exercises, and ask vendors to: (1) show that they have incident response plans and procedures as to the company; and (2) include the company in their plans, assessments and drills. This comprehensive approach will help parties on all sides prepare for and respond to incidents in a faster, coordinated, less expensive and more effective manner. Measures for effectively managing third-party risk are significant, and require foresight, energy and investment. Considering the magnitude of the risk, it is well worth a proactive approach.

**Judith H. Germano** is a Senior Fellow at the NYU Center for Cybersecurity and also the Center on Law and Security, and an Adjunct Professor of Law at NYU School of Law. She also is the founding member of Germano-LawLLC, advising companies and corporate boards on issues of cybersecurity, privacy, fraud, and regulatory compliance. Judith is the former Chief of Economic Crimes at the U.S. Attorney's Office for the District of New Jersey; a federal prosecutor for 11 years, Judith handled matters of cybercrime, securities and other financial fraud, political corruption and national security.

**The Center for Cyber Security (CCS)** is a non-partisan research Center at NYU focused on promoting interdisciplinary research, education, and programming focused on the most difficult cybersecurity problems of our time. The Center was founded as a collaboration between the Center on Law and Security at NYU School of Law and NYU's Tandon School of Engineering, and is led by Law faculty members Samuel Rascoff and Zachary Goldman, and Tandon faculty members Nasir Memon and Ramesh Karri.

