PROTECTING CONFIDENTIAL INFORMATION IN THE AGE OF CYBER ATTACKS: DO YOU HAVE A PLAN?

BY JASON M. STORCK, LAURA FAUBER, AND EDWARD HOLMAN

INTRODUCTION

With cyberattacks and the costs associated with data breaches increasingly on the rise, it is more important than ever for organizations to be prepared. Indeed, it is no longer so much a question of "if" an organization will become the victim of a cyberattack or other compromise of sensitive business, consumer, or employee information, but likely "when." Data breaches involving major organizations like Target, Home Depot, Kmart, and even the Democratic National Committee continue to make headlines, as do ever-evolving versions of ransomware attacks, such as WannaCry, which threaten to cripple an organization's ability to access critical data.

Guarding against—and mitigating the effects of—cyberattacks is of critical importance for organizations. Lax cybersecurity controls can adversely impact not only the privacy and trust of customers and employees, but also result in the loss of confidential business information, which can diminish the value and legal protection afforded to an organization's trade secrets. Moreover, significant data breaches can attract the attention of regulators, resulting in potentially significant fines and burdensome, long-lasting compliance obligations for organizations.

The good news is that there are practical steps organizations can take to greatly mitigate the risks of a cyberattack or other data breach. Indeed, as discussed below, many data breaches are not caused by malicious and determined outside actors, but simply human error or system glitches. By implementing basic controls like establishing an incident response plan, encrypting sensitive information, and training employees on security best practices, organizations can significantly reduce the potential impact of a cyberattack or data breach, as well as the associated costs, should one occur.

In this paper we examine why cybersecurity is important and provide an overview of the legal requirements involved. We then dive deeper into what constitutes a data breach, the potential adverse consequences for organizations that experience one, and how organizations should respond. Finally, we discuss how organizations can develop an effective cybersecurity plan, including an overview of effective security processes and controls, as well as essential internal policies and recommended employee training, assessment, and monitoring practices.

I. CYBERSECURITY OBLIGATIONS

A. Why is Cybersecurity Important?

It seems that with each passing week a new data breach makes news headlines in the United States. From restaurants like Chipotle[1] and Arby's,[2] and retailers like Brooks Brothers,[3] to hospitality providers like InterContinental Hotels Group[4] and Sabre,[5] and service providers

[1] https://www.chipotle.com/security (last visited Jun. 2, 2017).
[2] Brian Krebs, *Fast Food Chain Arby's Acknowledges Breach*, KREBS ON SECURITY (Feb. 9, 2017), https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/.
[3] Anya George Tharakan, *Retailer Brooks Brothers discloses payment card data breach,* REUTERS (May 12, 2017), http://www.reuters.com/article/us-brooks-brothers-cyber-idUSKBN1882QU.
[4] Brian Krebs, *InterContinental Hotel Chain Breach Expands,* KREBS ON SECURITY (Apr. 18, 2017), https://krebsonsecurity.com/2017/04/intercontinental-hotel-chain-breach-expands/.
[5] Brian Krebs, *Breach at Sabre Corp.'s Hospitality Unit*, KREBS ON SECURITY (May 2, 2017), https://krebsonsecurity.com/2017/05/breach-at-sabre-corp-s-hospitality-unit/.

like America's JobLink,[6] a wide variety of organizations have been impacted by data breaches already this year. Organizations affected by data breaches often face high financial costs, with the average cost to U.S. companies in 2016 estimated at $7 million per company, or $221 per record impacted.[7] These financial costs can be compounded by business and reputational costs that come along with being the target of negative front page news, major business disruptions and loss of data, a loss of customer trust, harm to brand image, and heightened scrutiny for any future missteps.

With real risks to consumers and employees in mind, federal and state regulators show no signs of easing off on enforcing cybersecurity requirements. The Federal Trade Commission (FTC), for example, has brought over 60 data security cases since 2002 against companies alleged to have put consumer's personal data at unreasonable risk, including recent actions against Ashley Madison,[8] ASUS,[9] D-Link,[10] Henry Schein Practice Solutions,[11] and Oracle.[12] State attorneys general also have been very active, entering into recent data breach settlements with companies like Target,[13] Acer,[14] Trump Hotel Collection,[15] and Adobe.[16] While not all settlements involve monetary penalties, larger breaches can sometimes draw fines in the millions of dollars, as shown by Target's $39 million and $18.5 million settlements with banks and states

[6] Mitchell Armentrout, *1.4M affected in data breach at Illinois employment department*, CHICAGO SUN TIMES (Mar. 29, 2017), http://chicago.suntimes.com/politics/1-4m-affected-in-data-breach-at-illinois-employment-department/.
[7] Ponemon Institute, *2016 Cost of Data Breach Study*, https://securityintelligence.com/cost-of-a-data-breach-2016/ (hereinafter *Ponemon Report*).
[8] Press Release, Federal Trade Commission, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.
[9] Press Release, Federal Trade Commission, ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.
[10] Press Release, Federal Trade Commission, FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras (Jan. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.
[11] Press Release, Federal Trade Commission, Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data (Jan. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled.
[12] Press Release, Federal Trade Commission, Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates (Dec. 21, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java.
[13] Press Release, The Attorney General of Texas, AG Paxton Announces $18.5 Million Settlement with Target to Resolve 2013 Data Breach (May 23, 2017), https://www.texasattorneygeneral.gov/news/releases/ag-paxton-announces-18.5-million-settlement-with-target-to-resolve-2013-dat.
[14] Press Release, New York Attorney General, A.G. Schneiderman Announces Settlement With Computer Manufacturer After Data Breach Exposed More Than 35,000 Credit Card Numbers, https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-computer-manufacturer-after-data-breach-exposed.
[15] Press Release, New York Attorney General, A.G. Schneiderman Announces Settlement With Trump Hotel Collection After Data Breaches Expose Over 70K Credit Card Numbers, https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-trump-hotel-collection-after-data-breaches-expose.
[16] Press Release, State of Connecticut Attorney General, AG Jepsen, Adobe Reach Agreement Resolving Connecticut-Led Multistate Investigation into Unauthorized Access to Servers (Nov. 10, 2016), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=587610.

Title search: Protecting Confidential Information in the Age of Cyber Attacks: Do You Have a Plan?

Also available as part of the eCourse
2017 Labor and Employment Law eConference

First appeared as part of the conference materials for the
24th Annual Labor and Employment Law Conference session
"Protecting Confidential Information in the Age of Cyber Attacks: Do You Have a Plan?"