Cybersecurity Best Practices

By Mandy Stanton, George Ernst and Anton L. Janik, Jr.

Stanton

Mandy Stanton Is a cyber security and privacy lawyer at the Mitchell Williams law firm where she co-leads the firm's Cybersecurity, Privacy and Data Protection practice.

Ernst

George Ernst is a partner at the Roberts Law Firm, where his practice includes Business Immigration Law, Employment Law and Cybersecurity Law.

Janik

Anton L. Janik, Jr., is a member of the Mitchell Williams law firm were he leads the Tax Controversy and Litigation practice and co-leads the firm's Cybersecurity, Privacy and Data Protection practice.

Over the last few years, it has become clear that threats to cybersecurity are only increasing, and therefore establishing sound cybersecurity risk-management polices and procedures will remain a critical consideration for businesses. From the recent headline-grabbing attacks on Target Stores, Home Depot, Subway, VISA, MasterCard, and JP Morgan Chase, as well as the Democratic National Convention email hack, the specter of cybersecurity threats and the potential for increased liability should be a concern for most businesses, especially in the retail, insurance, and banking industries. As a result of these threats, spending on cybersecurity initiatives totaled over $75 billion in 2015, and spending is expected to increase to $170 billion by 2020.[1] Indeed, nearly every company that collects or stores sensitive and confidential information is potentially at risk from cybersecurity threats. As businesses continue to use e-commerce and integrate networked information systems, these businesses become greater targets for cyberattacks.[2]

This article provides a general overview of the core issues and best practices that clients should consider to protect themselves from cybersecurity threats and the potential resulting liabilities. Given the multitude of variables, including the type of business, the agencies or commissions that regulate its business activity, and the type and method of data collected, this discussion will not be a "one-stop shop" for your clients. Moreover, because the threat landscape is constantly evolving and changing, it is important that your clients remain current, either seeking out or receiving from you updated information and advice as new threats, liabilities, and solutions become known. Due to this constantly evolving environment, we recommend that a corporate cybersecurity risk-management program be included in most businesses' administration plans, so that clients regularly reflect upon the potential hazards, their potential exposure, and the methods and means to combat them.

Determine Who Regulates the Clients' Activity

A particular difficulty when advising clients on cybersecurity risk-management issues is the lack of a clear and coherent omnibus or overarching set of cybersecurity laws and enforcement agencies. Indeed, the regulatory law establishing notification procedures and liability for a cybersecurity intrusion can stem from a variety of sectors and agencies, including, but not limited to, the Office for Civil Rights in the Department of Health and Human Services (HHS) for violations of the Health Insurance Portability and Accountability Act (HIPAA), the Consumer Financial Protection Bureau for financial consumer protection issues, the Department of Education for violations of the Family Educational Rights and Privacy Act, the Federal Communications Commission (FCC) for violations of the Telephone Consumer Protection Act, the Federal Trade Commission (FTC) for breaches of published consumer privacy policies, and even the Equal Employment Opportunity Commission (EEOC). Thus, when drafting and implementing a cybersecurity risk-management program, it is important to determine which agencies regulate the industry or the activity at issue, and thus which may be at your client's door in the event of a data breach, so that you can draft cybersecurity solutions, including a response plan, that takes into account and complies with those legal requirements.

> **"Implementation of an employee training arm in your data security plan is one of the best defenses against breaches. The Federal Trade Commission suggests creating a 'culture of security' ..."**

Perform a Vulnerability Assessment

Businesses and organizations should identify possible avenues of cybersecurity risk. Some of the more common examples of cybersecurity risks include permitting protected client or employee data to be accessed by or copied to insecure mobile devices in the bring-your-own-device ("BYOD") workplace or to be stored in insecure cloud computing environments. They also include the lack of appropriate controls and requirements with regard to employee social media usage, and the rise of the "internet of things," which refers to the increasing ability for everyday objects to gather data and connect to the internet. (For example, a home thermostat can cycle down your HVAC system when it detects you have left, and report to a mobile app that the owner is not at home. Transmitting data about whether a homeowner is home or away could create a security risk.) Clients should analyze their data collection methods and the security of same, considering how that data could be collected, and to what use it could be put. By analyzing and addressing these possibilities in light of the requirements set forth by the regulatory bodies governing that industry or that data, a vulnerability assessment will help your client understand the risks posed by their operation. However, it is important to remember that because new threats are ever evolving, regular cybersecurity vulnerability assessments searching for new and additional potential weaknesses should be part of a cybersecurity risk-management program.

Many businesses now require that their vendors perform vulnerability assessments. Many of our clients regularly insert cybersecurity warranties and cybersecurity audit requirements in their vendor contracts. Some clients accept vendor self-assessments while others require third-party audits, which may include penetration testing to provide reasonable assurances as to that vendor's ability to

keep data secure. However, identifying and remediating vulnerabilities does not necessarily mean reinventing the wheel. Several state and federal agencies have issued guidance documents for performing risk assessments, including the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.[3] The Federal Trade Commission has set forth guidance for testing for common vulnerabilities and in utilizing industry-accepted methods and technical and practice standards for securing data.[4] Regardless, in this environment of contractual cybersecurity requirements, timely vulnerability assessments can protect an organization, and also be an effective means to demonstrate to potential clients that cybersecurity risk-management is a corporate priority.

Keep Software Updated

A common but sometimes overlooked means to protect against cybersecurity threats involves incorporating a proactive policy of ensuring that all software is updated regularly and where appropriate.[5] Programmers regularly identify vulnerabilities in their software and issue patches for them in the form of software updates. Often, simply installing updates to software will eliminate or drastically reduce known vulnerabilities. Companies that do not update their software on a regular basis may leave unsecured known avenues for cybersecurity infiltration and data breach. Additionally, the failure to have a policy that requires software updates could lead to liability in the event of a breach that could have been prevented by the installation of a software update. Of course, many factors play into when a software update is installed, including the threat level of the potential harm, your client's vulnerability to that harm, and the other software your client uses that may not be compatible with that update. Therefore, it may be necessary to prioritize certain patches based on these or other considerations.

The Importance of Vendor Due Diligence and Contract Review

Delegating away responsibility for the risk that third-party vendors may lose your client's data is no longer an option, particularly in the healthcare and financial industries. A key component in mitigating third-party risk is to know your vendors and how their services affect your data security. Prior to selecting a vendor, it is important to clearly identify how the governing regulations impact the services in question, what legal responsibilities apply and how vendors implement those particular services.[6]

Due diligence should be conducted for any outsourced function,[7] although the depth of the investigations may vary depending on the scope of the services to be provided. Is an online search for publicly-available information about the vendor's cybersecurity precautions or a basic questionnaire sent to the vendor sufficient to quantify the potential risk this vendor may pose to your business and its data? Or would a more extensive search or vendor questionnaire or perhaps even an interview or site visit be more appropriate? Regardless, due diligence information should be verified and reviewed in context with your client's business goals and in consideration of the potential reputational impact a vendor may present.

Contract review is important to ensure that the client-vendor agreement is consistent with the client's business needs and complies with the client's cybersecurity risk-management program. In the context of data protection, some points to take into account when negotiating key provisions of a contract include:[8]

•Limitation of liability: What is the vendor's liability? Are the suggested limits, if any, reasonable given the scope of services and the information that may be impacted?

•Service levels: If a vendor fails to provide the service level standard (e.g., incident response times, data encryption usage) as provided for in a contract, does that potential failure impact data protection? If so, what is the impact?

•Data protection: Are contractual security requirements specific and measurable for acceptable performance? Is confidentiality as well as security covered? Are any relevant types of data excluded from certain protections? Are there industry standards that can be incorporated to provide acceptable protection?

•Termination for Convenience: Are expectations set up front regarding whether a breach of confidentiality, security or failure to comply with applicable law triggers a termination right?

Mitigating vendor risk doesn't end when the ink dries on the contract. Periodic contract reviews, especially as contract renewals arise, and ongoing monitoring based on the most current legal requirements or other applicable regulatory or industry standards should play an integral part in vendor management. In addition to evaluating performance, monitoring should also consider any mitigation agreed to in the contract, such as service levels and data security clauses.[9] Also, being mindful of news headlines and performing regular online searches of your vendors may provide valuable information.[10]

Control Access to Data with an Access-Management Plan

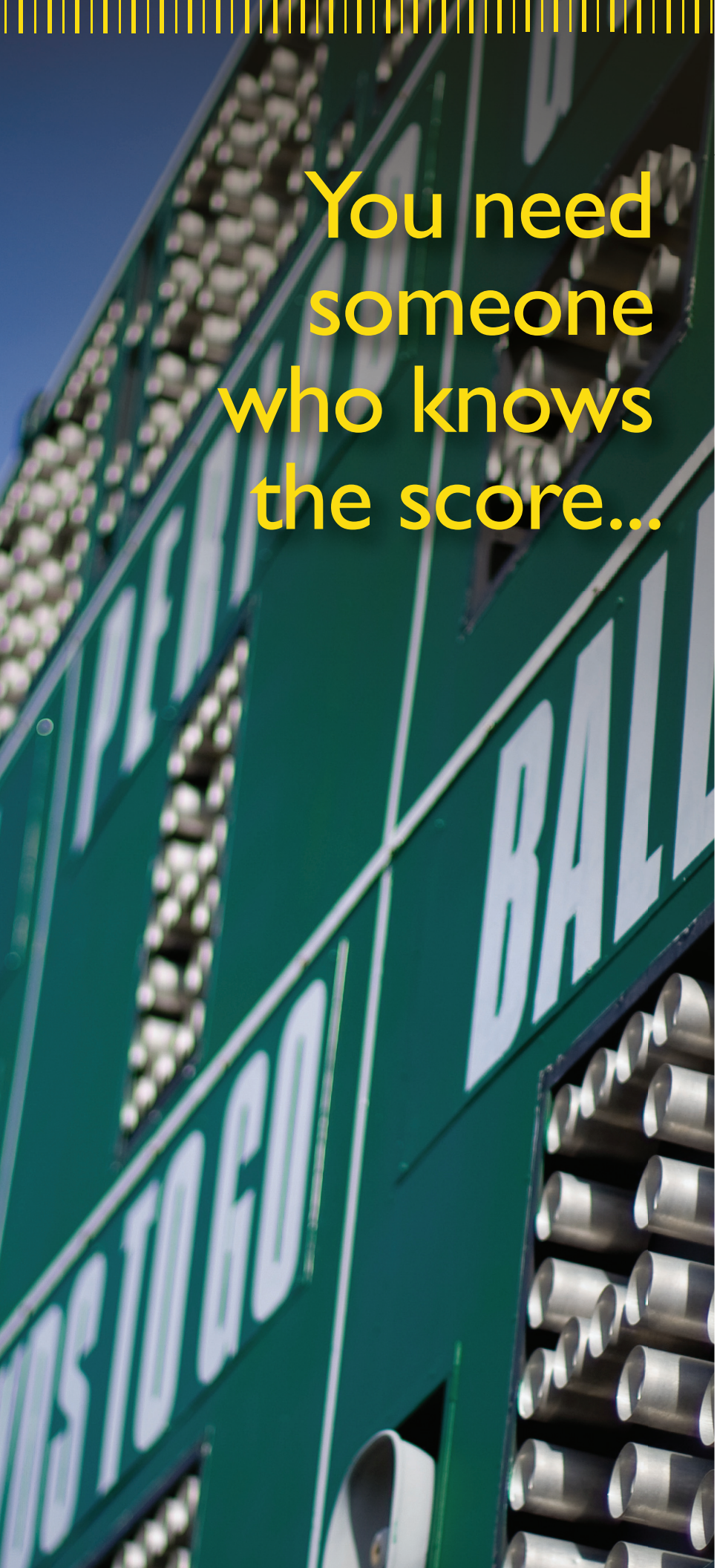
Controlling access to data with an access-management plan should be an integral piece of a cybersecurity risk-management policy. An effective access-management plan should establish the "when and how" of employees' access to information and networks,[11] while keeping within the context of the business's goals and the legal or ethical responsibilities of the organization. General consideration should be given to the following:

•At what point should access be acquired?
•How long should access be retained?
•When should access be terminated?
•Should access to certain files or applications be restricted?
•Is there a system for limiting or restricting virtual access to an organization's files on an as-needed basis?
•Which employees should have administrative access to an organization's systems?
•Are there limits to third-party access to an organization's network?
•Can you encrypt financial and personally identifiable information?

The Federal Trade Commission further recommends controls for information access such as restricting access to network information, separate user accounts where personal data is stored and locking file cabinets.[12] You should also consider whether there are contractual obligations to consider when determining the parameters of information access. Most non-disclosure and confidentiality agreements contain standard language that the parties agree to share information within the organization on a need-to-know basis and/or only to the extent necessary to perform their obligations.

Regular Employee Training is Vital

Multiple studies and research point to



You need someone who knows the score...

...whose strategy is forged from depth of experience. Associate the unique expertise of The Law Office of David H. Williams for complex medical and product defect cases, including:

Prilosec®, Prevacid®, and Nexium®

these heartburn drugs can increase the risk for developing kidney disease

Invokana®

this diabetes drug is linked to kidney failure and diabetic ketoacidosis

Levaquin® and Avelox®

these antibiotics are linked to aortic aneurysms and/or dissection, as well as peripheral neuropathy

IVC Filters

these vena cava filters which are inserted IV can detach and fracture leading to migration and perforation

Talc

is found in Johnson & Johnson Baby Powder and Shower to Shower products and is associated with the development of Ovarian Cancer

Xarelto®

this anticoagulant marketed by Bayer and Johnson & Johnson may increase the risk of stroke, blood clots and internal bleeding

THE LAW OFFICE OF
DAVID H. WILLIAMS

David H. Williams

211 S. Spring Street
Second Floor
Little Rock, AR 72201
(877) 492-3030
(501) 372-0038
david@dhwlaw.net
dhwilliamslawfirm.com

PRESERVE
THE JURY TRIAL

employees as the leading cause of data breaches. Implementation of an employee training arm in your data security plan is one of the best defenses against breaches. The Federal Trade Commission suggests creating a "culture of security" through communication of policies, training on a regular basis, identifying clear reporting channels and implementing such policies and procedures in a consistent and active manner.[13] As part of that culture, it is important to designate a privacy officer to implement a security strategy and counsel on processes and procedures involving privacy and security. When developing your employee cybersecurity training program, consider the following elements:

•Communication: Are your cybersecurity policies communicated regularly through initial hire training, organization-wide training on a regular basis, and in employee policy manuals or handbooks?

•Training: Are you conducting training on a regular basis? Is this training updated as technology, threats, policies or other considerations evolve?

•Reporting Channels: Are reporting channels clear, simple and easily accessible?

•Active Implementation: Is employee compliance being monitored? Are disciplinary measures imposed for violating security policies? Are employees that identify vulnerabilities publicly acknowledged?

•Testing: Do you regularly test your employees' ability to detect and report on cybersecurity threats like phishing emails?

Typically, it is not the lack of leadership, knowledgeable staff or funding that creates a barrier to a strong security culture. Rather, it is insufficient planning, and a lack of regular training and across-the-board preparedness.[14] Taking the time to make employee cybersecurity education a priority is widely considered to be time well spent.

Create a Cybersecurity Breach Response Plan

A well-defined breach response plan is vital to an orderly and successful response. A breach response plan should identify the personnel, including a privacy officer having responsibility to investigate, analyze, respond, issue required notifications, and respond to public inquiries about the event, as well as set forth any necessary timelines or protocols for carrying out the plan. The plan should be regularly reviewed and if possible, test implemented, with the identified persons taking part.

Know Your Notification Requirements

Although all clients want to prevent a cybersecurity breach from ever happening, the odds are that one will still occur. If a breach occurs, it is important to determine whether the client is required to provide notification to the persons whose data has been compromised. Currently, 45 states (including Arkansas), the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted security breach notification statutes.[15] A breach of a security system means the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business."[16]

Under Arkansas' law,[17] generally, "[a]ny person or business that acquires, owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[18] Personal information includes an individual's first name or first initial and last name in combination with another data element (social security number, driver's license number, account or card number and pass code, or medical information). If that occurs, the notice must be made in the most expedient time and manner possible and without unreasonable delay. To ensure full compliance, and to determine whether any exemptions are available from this general rule, it is important to encourage clients to discuss any instances of a data breach as soon as possible. Additionally, it is important to note that should a client maintain records for individuals who live in other states, it is important that the client's data breach response plan also address the notification requirements of those other states.

This article has covered a broad scope of considerations, but not all may apply to your client's business. However, the regular examination of the cybersecurity risk-management concerns that do apply to your client's business is vital to its continued success, and should therefore be an ongoing component of your client's business plan.

Endnotes:

1. http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#3c69faf22191.
2. Ronald N. Weikers, Data Sec. & Privacy Law § 1:3 (2016).
3. https://iapp.org/media/pdf/resource_center/Krasnow_model_WISP.pdf.
4. https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
5. *Id.*
6. https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/.
7. https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.
8. https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/.
9. Kirkpatrick, Brian, *Legal Ethics: Cybersecurity in Your Daily Practice,* http://westlegaledcenter.com/program_guide/course_detail.jsf?courseId=100104131.
10. https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/.
11. https://iapp.org/news/a/designing-and-implementing-an-effective-privacy-and-security-plan/.
12. https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
13. https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.
14. Ponemon Institute, *The Cyber Resilient Organization: Learning to Thrive against Threats*, http://www.ponemon.org/library/the-cyber-resilient-organization-learning-to-thrive-against-threats (last visited March 3, 2016).
15. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
16. Ark. Code Ann. § 4-110-102(1)(A).
17. Ark. Code Ann. § 4-110-101, *et. seq*.
18. Ark. Code Ann. § 4-110-105(a)(1). ■