Message from the Chair

Dear Cyberspace Colleagues:

It's nearly impossible to open a newspaper-paper or digital-and not see a headline related to the issues cyberspace lawyers address every day. Never has our work seemed more relevant! As you endeavor to answer the needs of your clients (companies, employers, or students), access the rich resources the Cyberspace Law Committee provides.

Come join your Cyberspace colleagues to learn from each other at the BLS Spring Meeting next month, April 12-14, in Orlando. See the article below for our full agenda and descriptions of the three CLE programs we are sponsoring. Many thanks to John Black, Steve Middlebrook, and Tsui Ng for coordinating these programs. And participate in our committee and subcommittee meetings to get involved with our work-books, webinars, in-person CLE programs, and more. We always welcome new ideas!

Remember that, if you missed the 2018 Cyberspace Law Institute, you can still access some of the material shared through the meeting webpage.

If your circumstances make it difficult for you to join us at BLS and standalone committee meetings, we have a great opportunity for you to collaborate through our Current Law Task Force, which tracks and reports on recent developments in cyberspace law and serves as an incubator for publications and presentations. The task force, chaired by Michael Silvestro, can help you publish works of varying length and detail, ranging from long-form articles to pieces as brief as one paragraph. Join the task force on its webpage to get on the listserv and learn about the monthly calls.

Please let Cheryl Burtzel or me know how you would like to get involved!

Cheryl Dancey Balough
Chair, Cyberspace Law Committee

Your Work on ABA Projects Can Impact National Discussions

Your work with the ABA can have an impact on the discussion of national cyberspace issues. In prior issues of this newsletter, we have highlighted the work of committee members Cheryl M. Burtzel, Candace M. Jones, and Lisa R. Lifshitz. These committee members co-authored (along with Lucy Thomson of the Science and Technology Committee), a work entitled Vendor Contracting Project: Cybersecurity Checklist.

Recently, this ABA publication was referenced in a report entitled The Cost of Malicious Cyber Activity to the U.S. Economy, released on February 16, 2018 by The Council of Economic Advisors (CEA), an agency within the Executive Office of the President of the United States. Find the CEA’s press release here.
If you haven't registered for the BLS Spring Meeting, there's still time. Cyberspace Law Committee will have a full day of committee and subcommittee meetings on Thursday, April 12, and we are sponsoring three CLE programs. Given the strength of our committee's contributions, we have some overlap, but we do not take offense if you split your time between two concurrent meetings. Here's our schedule:

**Thursday, April 12**

8:00 - 9:00 am: Cyber Insurance Subcommittee Meeting, Cross-Border E-Commerce Subcommittee meeting
9:30 - 11:00 am: Cyberspace Law Committee Meeting
11:00 am - Noon: Consumer Privacy & Data Analytics Subcommittee Meeting, Smart Contracting Subcommittee Meeting
Noon - 1:00 pm: Publications Subcommittee Meeting, Robotics & Artificial Intelligence Subcommittee Meeting
1:00 - 2:00 pm: Cybersecurity Subcommittee Meeting
2:00 - 3:00 pm: Financial Services and Payments Subcommittee Meeting, Healthcare IT Subcommittee Meeting
2:00 - 3:30 pm: "Cyberinsurance: Coverage, Claims and Cross-Border Concerns"
This panel will discuss the insurance coverage, claims and emerging issues in cyber insurance in the U.S. and EU, discussing the effect of the GDPR, cross-border concerns and the disparate cyber risks faced by different types of businesses, such as healthcare, financial institutions, professional organizations and manufacturers.
3:00 - 4:00 pm: Cloud and Enterprise Technology Subcommittee
4:00 to 5:00 pm: Non-US Cyber Regulations Subcommittee Meeting, Internet Governance Task Force Meeting
7:00 to 10:00 pm: Cross-Committee Dinner

**Friday, April 13**

10:30 am - Noon "Legal Issues Arising from the Use of AI to Provide Financial Services"
This panel will provide an overview of how AI is being used in financial services, discuss how regulators may view the new technology and identify the legal and compliance issues that business lawyers should look for in AI projects. An important topic will be so-called "algorithmic bias," or the potential for unintentional discrimination to creep into the AI process. The panel will offer perspectives on how financial services providers can monitor for algorithmic bias and prevent potential UDAAP violations.
2:30 - 4:00 pm "What's Lurking Back There: Cybersecurity Risks in Legacy Systems"
This panel will discuss risks associated with outdated legacy systems that are still pervasive across industry and government. After addressing the systems roles in many high-profile data breaches, the panel will offer tips on how to manage those associated risks while migrating to new systems.

You can access the full agenda [here](https://aba.libraries.chicago/BBIBZ/Teamsite/buslaw/committees/CL320000pub/newsletter). If you have already registered, please revisit your reservation to purchase a ticket to our Thursday evening dinner. (Click on "Register Now" and then "View/Edit Reservation"). Join us for a casual, fun time with our colleagues in several other committees.
The Cyberspace Law Committee is pleased to sponsor the following CLEs next month at the BLS Spring Meeting:

**Cyber Insurance: Coverage, Claims, and Cross Border Concerns:**

*Thursday, April 12, from 2:00 pm - 3:30 pm*

In the wake of very public data breaches and malware attacks, cyber insurance has become an important tool in a modern organization's arsenal to defend its operations and confidential information from cyberattack. However, the protections afforded by cyber insurance sometimes are not well understood because policies are not standardized and can be complex and technical. Moreover, understanding the scope of such coverage can be even more challenging in light of evolving cyber risks that organizations face. Criminals, hacktivists, rogue employees and nation-states relentlessly seek to exploit vulnerabilities within organizations to disrupt business operations and steal valuable trade secrets, personal information and money. The recent adoption of laws and regulations such as the EU General Data Protection Regulation ("GDPR") introduces further uncertainty for organizations as they strive to address new legal obligations and exposures.

Against this backdrop, a panel comprised of cyber insurance professionals and lawyers will address these developing business and legal issues and the protection that may be afforded under cyber insurance. The panel, which includes cyber insurance underwriters from two major insurers, a senior cyber claims representative from a major insurer, a cyber insurance broker, and U.S. and EU attorneys who deal with privacy law and cyber insurance and claims, will discuss the nature and scope of insurance currently available for cyber risks and describe the claims that have arisen under cyber insurance. Following this, the panel will examine the likely impact of the GDPR on data privacy exposures facing U.S. and EU organizations and the cyber insurance coverages available for emerging cyber exposures including for the new obligations imposed by the GDPR.

**Legal Issues Arising from the Use of Artificial Intelligence to Provide Financial Services**

*Friday, April 13, from 10:30 am - 12:00 pm*

Financial institutions and service providers are beginning to use Artificial Intelligence (AI) technology to monitor for fraud, verify customer identity, provide customer service, make credit determinations and offer robo-advising services. The adoption of this new technology raises a number of novel legal questions.

This panel will provide an overview of how AI is being used in financial services, discuss how regulators may view the new technology and identify the legal and compliance issues that business lawyers should look for in AI projects. An important topic will be so-called "algorithmic bias," or the potential for unintentional discrimination to creep into the AI process. The panel will offer perspectives on how financial services providers can monitor for algorithmic bias and prevent potential UDAAP violations.

Speakers: Stephen T. Middlebrook, Womble Bond Dickinson; Alexandra Villarreal O'Rourke, McGuire Woods; David A. Stein, Covington

**What's Lurking Back There: Cybersecurity Risks in Legacy Systems**

*Friday, April 13, from 2:30 pm - 4:00 pm*
A legacy system is a system, which may be in use, but is outdated or no longer supported by the developer. Legacy system threats are pervasive across many industries - corporations, infrastructure, government, and financial services. Examples of data breaches that can be traced back to legacy system vulnerabilities include Equifax, Home Depot, and OPM. We will discuss the risks associated with legacy systems, including patching and updates. We will also evaluate best practices for managing legacy system risks while adopting new technology, including due diligence and integration with interconnected systems.

Program Chair: Tsui Ng; Attorney, NYC Department of Education

Materials Coordinator: Jordan Fischer, Xpan Law Group

Moderator: Candace Jones, Federal Reserve Bank of New York

Speakers: Michael Fleming, Cray Inc.; David Flint, MacRoberts LLP; Lisa Lifshitz, Torkin Manes LLP

---

Subcommittee News

From the Consumer Privacy and Data Analytics Subcommittee

The Consumer Privacy and Data Analytics Subcommittee (CPDAs) is continuing its preparations for a major project. The one idea that has received the most traction is the creation of a checklist of considerations for organizations in the privacy and data analytics space. Thus far, we have recruited the following contributors:

1) Erin Illman - the U.S. privacy perspective;
2) Juliette Moringiello - Will advise CPDAs on current other ABA checklist projects we can peruse for ideas on what an end product would look like;
3) John Isaza - the EU privacy perspective.

Besides the above three contributions, CPDAs still needs volunteers on the following:

1) Asia perspective
2) Latin America perspective
3) Eastern Europe perspective
4) Data analytics concerns

Since the project is still in its early stages, we welcome input. This project may grow or constrict organically, so for the time being please feel free to submit ideas to either John Isaza or John Rothchild.

Once we have a project under way, CPDAs will set up a team room to collaborate on the actual project. Also, depending on interest, CPDAs may schedule a conference call or two before the Spring ABA Conference in Orlando. For those who will not be able to attend the Spring Conference, CPDAs will facilitate a conference line to call-in and participate virtually.

From the Current Law Task Force

Are you interested in writing about emerging topics in cyberspace law? Would you like to publish a piece on a recent development, but don't have the time to draft a long article? Are you looking for a way to get more involved with the Cyberspace Law Committee without traveling to a meeting?

If so, call in to the next meeting of the Cyberspace Law Committee's Current Law Task Force on Wednesday, March 14 at 10:30 am CT/11:30 am ET. New members are always welcome.
The Current Law Task Force tracks and reports on recent developments in cyberspace law and serves as an incubator for publications and presentations. There are a variety of available publication opportunities, including contributions to the Cyberspace Law Committee Newsletter and Business Law Today. The Task Force can help you publish works of varying length and detail, ranging from long-form articles to pieces as brief as one paragraph.

The Current Law Task Force meets through monthly conference calls to discuss new developments and ideas for publications. The dial-in information for the call is below:

Call In: 312-667-9356
Conference ID: 079455
Security Pin: 160049

From the Cross-Border E-Commerce Subcommittee

The Cross-border e-Commerce subcommittee held two conference calls in February to discuss the cloud computing work on the April agenda of the UNCITRAL Working Group on e-Commerce. The second call was joined from Vienna by the principal legal officer of that Working Group. Notes from the call will be provided to the Secretariat for its consideration.

Notices will be sent to members of the subcommittee through the listserv, about future calls. We may want to consider the implications for our clients of the Supreme Court's hearing (and disposition, ultimately) of the Microsoft subpoena case. What does it tell us about our clients'-or our own-obligations to keep records under the legal systems to which they may be exposed?

In addition, the Subcommittee plans a future call on the other UNCITRAL agenda item for April, identity management, once the working paper on that topic becomes available.

Later this spring, it will also-as is its custom-review recent international initiatives affecting U.S. and other business interests in e-commerce.

Calls are usually joined by knowledgeable members of the Section of Science and Technology Section as well.

What Can Directors and Officers Learn from Ransomware Attacks?

Richik Sarkar, Member, McGlinchey Stafford PLLC

Courts have historically set a high threshold to find directors and officers personally liable for breaches of fiduciary duties. However, high stakes and increased publicity will likely cause director and officer liability standards for damages resulting from cyberattacks and data breaches to evolve, and personal exposure of directors and officers will increase.

To wit, in September 2015, following Home Depot's high-profile data breach, a shareholder derivative lawsuit was filed in the Northern District of Georgia against 12 Home Depot directors and officers. The suit broadly alleged breaches of the "fiduciary duties of loyalty, good faith, and due care" because officers and directors "knowingly and in conscious disregard of their duties [failed] to ensure that Home Depot took reasonable measures to protect its customers' personal and financial information" in advance of the data breach.

Read more...
Proposed Texas Class Action Based on Driver’s Privacy Protection Act Moves Forward


On January 4, 2018, United States District Court for the Northern District of Texas Dallas Division issued a Memorandum Opinion and Order by Judge Jane Boyle in the Arthur Lopez (Lopez) versus Don Herring Ltd. (Herring) case: Civil Action No. 3:16-CV-02663-B. Lopez filed a Driver's Privacy Protection Act (DPPA) class-action claim after Herring, a car dealer, mailed Lopez—and potentially others—an advertisement that detailed what Lopez believes to be information gained from the Texas Department of Motor Vehicle's. Initially other defendants were included in the DPPA claim but only Herring remains; Herring attempted to have the case dismissed based on Federal Rule of Civil Procedure 12 (b) (6), but Judge Boyle denied Herring's motion.

Blockchain Law & Technology Symposium

Sarah Jane Hughes will be attending and presenting a draft of a new paper at Cleveland State Law School's Cleveland-Marshall Law Review's Blockchain Law & Technology Symposium on April 6, 2018.

Call for Future Contributions

Do you have something that might make a good contribution to next month’s Cyberspace Law newsletter? Email Tom Kierner with your blurb! Have a longer or less Cyberspace-y contribution? It might be a good fit for Business Law Today. Email Juliet Moringiello and she will help you with the submission process.
What Can Directors and Officers Learn from Ransomware Attacks?  
Four Questions to Consider to Minimize Exposure

Richik Sarkar, Member, McGlinchey Stafford PLLC

Courts have historically set a high threshold to find directors and officers personally liable for breaches of fiduciary duties. However, high stakes and increased publicity will likely cause director and officer liability standards for damages resulting from cyberattacks and data breaches to evolve, and personal exposure of directors and officers will increase.

To wit, in September 2015, following Home Depot’s high-profile data breach, a shareholder derivative lawsuit was filed in the Northern District of Georgia against 12 Home Depot directors and officers. The suit broadly alleged breaches of the “fiduciary duties of loyalty, good faith, and due care” because officers and directors “knowingly and in conscious disregard of their duties [failed] to ensure that Home Depot took reasonable measures to protect its customers’ personal and financial information” in advance of the data breach.

On April 28, 2017, the parties filed a proposed settlement to resolve the matter, which, if approved, would require Home Depot to change its governance structure, reorganize risk management entities, and pay the shareholders’ attorneys more than $1 million, among other things.

While case law might suggest that personal liability findings against officers and directors are unlikely, the reputational risk and indirect financial implications of losing a job or board seat cannot be quantified. And the CryptoLocker, WannaCry and NotPetya attacks made real the harrowing threats for those at the helm of an organization of such attacks: the high cost of data recovery; hours and days of downtime; and, in the worst case, criminals taking control of a company’s intellectual property — to be sold or publicly released at another’s whim.

These and other cyber risks can affect the operations and intrinsic value of an organization, and, as the rate of litigation against directors and officers increase, can be very costly for officers and directors. See, Sharp Rise in D&O Litigation Signals Change in Legal Strategy. These and other matters have put all directors and officers on notice: Those who underestimate the personal risk associated with cybersecurity and data privacy issues do so at their peril.

What Are Directors’ and Officers’ Fiduciary Duties With Respect to Cybersecurity?

Officers and directors typically know their fiduciary duties and their Business Judgment Rule protections — a presumption that in making a business decision, the officers and directors of a corporation act on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the company. As stated in the seminal In re: Caremark International, Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996), “a director’s obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances, may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.”

With respect to cybersecurity issues, courts and regulators will employ stringent standards and specifically analyze how boards are identifying, assessing, and addressing cyber risk. Thus, proper board preparedness and planning are critical to insulating officers and directors from liability.

In Palkon v. Holmes, 2014 WL 5341880, D.N.J., Oct. 20, 2014, a federal district court dismissed a shareholder class action against directors, the president/CEO, and general counsel of Wyndham Worldwide
Corporation. The class action alleged breaches of the fiduciary duties of care and loyalty, and the wasting of company assets following three data breaches between April 2008 and January 2010 that resulted in the theft of more than 600,000 customers’ credit card information. The Business Judgment Rule was critical to the court’s decision making, finding that the rule protected the board because it:

- Held 14 quarterly meetings in which it discussed the cyber attacks, company security policies, and proposed security enhancements.
- Appointed an audit committee, which met at least 16 times to review cybersecurity and to investigate breaches.
- Hired a technology firm to recommend security enhancements, which the company had begun to implement.
- Had cybersecurity measures in place that had been discussed numerous times by the board prior to the security breach.

_Palkon_ provides an objective standard of what will protect directors and officers: Boards must hold frequent meetings—at least quarterly—to analyze cyber risks and potential plans of actions. They should create or appoint a committee to review cyber issues and/or investigate data incidents and breaches. They should seek third-party guidance with respect to assessing and implementing security enhancements, and must understand what cyber risks can affect their entities and have a clear plan to address risks. In short, boards must implement a cyber risk management program; oversee and test the program; and, investigate possible threats and actual breaches.

On the other end of the spectrum, and much more subjective, is the analysis of the Third Circuit Court of Appeals in _In re: Lemington Home for the Aged_, 777 F.3d 620 (3d Cir. 2015), which, while not a data breach case, provides a cautionary tale for all officers and directors. In that case, the Third Circuit upheld an extremely rare finding of personal liability fiduciary breaches because the directors did not exercise reasonable care: allowing underperforming and unqualified officers to remain in their roles and failing to remove them once the results of their mismanagement were made clear.

The Third Circuit recognized that, while directors and officers can rely on information, opinions, or reports prepared by others, they do not act in good faith when they have knowledge of a situation that would cause their reliance to be unreasonable: “[t]his was not a case where directors, acting in good-faith reliance on ‘information, opinion, reports or statements’ prepared by employees or experts, made a business decision to continue to employ an Administrator whose performance was arguably less than ideal...” Rather, the directors in this case had “actual knowledge of mismanagement, yet stuck their heads in the sand in the face of repeated signs that residents were receiving care that was severely deficient.”

_In re: Lemington Home for the Aged_ is completely consistent with the controlling analysis of _In re: Caremark_, which noted that “only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information reporting system exist —will establish the lack of good faith that is a necessary condition to liability.” And the Third Circuit’s exacting analysis subjected those officers and directors to immense personal liability for failing to properly identify, detect, and protect the entity from organizational risks before they occurred, and for their failure to properly respond when such failings were exposed.

It is not a great leap to assume that similar standards—and liability—will be applied to officers and directors if they fail to properly identify, detect, and protect firms from cybersecurity risks before they occur, and for failure to properly respond when such cybersecurity failings are exposed. To create a spectrum, _Palkon_ establishes how officers and directors can protect themselves and organizations from liability. _In re: Lemington Home for the Aged_ demonstrates what can happen if proper cyber risk management and security protocols are not put in place and consistently monitored by management and the board.
Without question, once data breaches and cyberattacks are discovered, boards and management have a duty to investigate. And, while such investigations can be internal, they are best handled by independent, outside legal counsel for two reasons: (1) to cement attorney-client privilege, protecting critical and confidential information and analysis from discovery; and (2) to further establish good-faith efforts to discharge their fiduciary duties.

How Can Officers and Directors Properly Discharge Their Cybersecurity Fiduciary Duties?

Once on notice of compliance or risk management issues (either constructively or actually), if a board determines in good faith no further action is warranted, the Business Judgment Rule should protect such decision. However, if there is no formal process and/or only a cursory internal process is utilized, Business Judgment Rule protections may not apply as “the presumption created by the Business Judgment Rule can be rebutted only by affirmative allegations of facts which, if proven, would establish fraud, bad faith, overreaching, or an unreasonable failure to investigate material facts.” Berg & Berg Enterprises v. Boyle, 178 Cal. App. 4th 1020, 1046 (2009). When addressing the level of cybersecurity awareness expected from board members, Securities and Exchange Commission Commissioner Luis Aguilar observed in June 2014:

Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyberattacks. To that end, board oversight of cyber risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.

Commissioner Aguilar also noted that the National Institute of Standards and Technology (NIST) Cybersecurity Framework created an industry standard that corporations, directors, and officers could incorporate into their plans to be proactively address the occurrence of a possibly devastating cyber event. To summarize the requirements of the NIST Cybersecurity Framework (to the extent any article can), the hallmarks of truly effective cyber-risk governance strategy includes:

- **Defined roles for directors and management.** Defining clear roles for management, board committees, and individual directors ensures protocols are developed and deployed cost-effectively.

- **Constant assessment of cybersecurity plans, trends and threats.** To ensure Business Judgment Rule protection, it is wise to have regular presentations for pertinent committees to provide updates on trends and threats. Having outside counsel lead this process can allow attorney-client privileges and protections to take hold and protect critical deliberations from disclosure.

- **Cybersecurity vigilance permeates the organization.** Employees, vendors, and partners must receive continuous education to create a culture of cybersecurity.

- **Continually evolving cyber preparedness plans and controls.** Organizations must incorporate systematic threat and weakness assessments into their cyber risk management plans and modify established programs and protocols as required.

- **Detailed incident response plans and protocols.** An effective program assesses the type and scope of the incident and what critical information has been accessed or misused to prevent further unauthorized access to or misuse. It also establishes business continuity protocols and public relations and/or crisis communication plans involving counsel, consultants, and the company insiders. Finally, it should provide a plan to determine whether law enforcement should be noticed.
- **Comprehensive insurance coverage.** While an industry standard is slowly emerging, gaps between first- and third-party coverage under existing policies may result in uncovered losses. Pay attention to whether coverage applies to attacks over time (which occurs in many situations) as opposed to specific events. To that end, firms should also conduct a comprehensive review of their policies to determine what cyber risks are covered and which of the four typical cyber liability insurance policies should be purchased.

To further highlight the importance of cyber insurance specifically, risk managers and boards must understand insurance policy variations and their implications, such as requiring cybersecurity specialists or attorneys to assess potential policy gaps, blind spots, etc. To that end, the insurance purchasing process can be useful, as determining appropriate coverage often requires completing questionnaires about a firm’s data security practices and procedures. This can provide a snapshot of a company’s data security risks and practices. More importantly—as carriers often require that board and management will ensure that policies and procedures continue to be in place as a condition of the coverage—boards overseeing this process should work with consultants to ensure that claims cannot be denied because of incomplete or inaccurate applications.

Considering the myriad of cybersecurity risks and concerns — with directly related fiduciary duty and director liability issues—only a comprehensive, multidisciplinary approach involving the integration of multiple legal specialties and service teams can provide public, private, and nonprofit directors with the proper strategy and tactics to address cybersecurity risks while enhancing officer and director protection. It is also critical to note that insurance companies, regulators, and shareholders, even in close corporations, will expect firms to view publicized cyber events such as WannaCry as teaching and learning moments, even if their entities were not attacked. Learn from the Palkon example: engaged board members and committees can help cement the Business Judgment Rule protections. And learn from the mistakes in In re: Lemington Home for the Aged: a perfect plan is useless if it is simply in a drawer.

**What Is The Potential Exposure for Directors and Officer As the Result of Cyber-Incident?**

As the number of data breaches grows, the potential liability for officers and directors grows as well. Cases had been trending toward finding alleged damages too remote to establish liability. See, e.g., Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017) (affirming dismissal where the consumer did not suffer any concrete injury following the company merely holding his personal information for 8 years after commercial relations ended, and Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (affirming dismissal for lack of standing for consumers’ failure to establish a non-speculative future harm). However, some courts are reversing course, allowing cases to move forward and causing risk of unfavorable judgments to increase. One of the more significant rulings in this line of cases is Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir., May 2015), where the Seventh Circuit Court of Appeals found that “the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identity” and determined that the class “should have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an ‘objectively reasonable likelihood’ that such an injury will occur.” The Seventh Circuit’s finding that likely future harm is sufficient for standing is significant as it has arguably reduced the standing barrier and more consumer and shareholder derivative data-breach lawsuits will likely survive initial dismissal attempts, increasing risks for entities and their boards. See also, Lewert v. P.F. Chang’s, 819 F.3d 963 (7th Cir. 2016) (finding standing for future injuries based on stolen data); Galaria v. Nationwide Mutual Insurance Company, 663 Fed. Appx. 384 (6th Cir. 2016) (holding that consumers do not have to wait for stolen data to be used to have standing).

Sadly, it is a near truism that with increased regulation comes increased litigation. Thus, more than ever, data breaches and attacks will trigger subsequent state or federal regulatory actions, shareholder
derivative actions, and/or other claims against directors and officers for injuries to the organization. Though the unsettled nature of standing is disconcerting, the legal liability associated with data breaches can pale in comparison to business effects such as damaged reputation, lost customers, data loss, business continuity issues, loss in shareholder value, and lost jobs. Further, equity funds and companies considering acquisition and investment now consider cyber preparedness; a lack of plans will impact the value and a business' potential sale price. It is not a stretch to imagine that some potential company sales were hindered because the target did not weather the WannaCry storm. Cybersecurity is clearly not just an IT issue, but rather a corporate strategy issue that affects everything: information, profits, assets, and executives.

**How Can Officers and Directors Reduce Their Risks?**

Board and officer level cyber preparedness is the only way to ensure that cybersecurity issues do not disrupt business continuity, decrease business valuation, and adversely affect the business reputation of the company and its officers and directors. To protect against personal exposure resulting from potential cyber risk requires a shift of traditional fiduciary analysis from questions of liability and defense to questions of offensive and proactive stewardship. To this end, companies, at the direction of the board, and preferably led by counsel, to ensure maximum protection, should:

- Deliberately and consistently educate directors about industry best practices and, more importantly, the company’s cybersecurity policies, controls, and procedures, including:
  - Critical cyber assets and threats
  - Existing controls and programs
  - Third-party vendor management
  - Development and implementation of a cyber incident response protocol
  - Insurance coverage
  - Business continuity plans
  - Appointing officers and directors with expertise in cybersecurity issues

- Create company departments and/or board committees to be primarily responsible for data privacy and cybersecurity issues
- Conduct regular officer and director meetings to ensure that the company’s expectations and processes are being diligently followed
- Investigate possible violations once the board has actual or constructive notice of compliance and risk management issues (through whistleblowers, formal and informal complaints, regulatory inquiries, etc.)

In short, officers and directors must take the initiative and, working with attorneys and consultants, directly address cybersecurity and ensure protocols and procedures are incorporated into a company’s overall business strategy and corporate culture.