As legal counsel advising governing bodies, boards or trustees, public pension plan attorneys need to be cognizant of the increasing level of responsibility by trustees for cybersecurity oversight. Information and information systems are critical assets for any business, including pension plans. Plans collect and maintain highly coveted personal information about members and beneficiaries, as well as financial data. Legal and regulatory developments highlight the importance of data as a business asset and place cyber risk high on an organization’s risk management and oversight responsibilities. What has also become abundantly clear is that cybersecurity is no longer solely an IT department responsibility.

Cyber attacks are an ever-growing and changing threat, with public announcements revealing breaches of an organization’s confidential data becoming more frequent each year.1 Given the significant costs associated with responding to a large breach, the importance of the data contained within an organization vulnerable to an attack, and the rapidly changing risk profile associated with the type and sophistication of new cybersecurity threats, ensuring the adequacy of an organization’s cybersecurity measures should be a crucial part of a board’s risk oversight responsibilities.

The Maturing Cyber Risk Landscape

The United States Government Accountability Office (GAO), in its 2015 report to congressional committees, noted the continued increase of cybersecurity incidents to systems supporting the federal government over the past decade. According to the report, the number of incidents over a fiscal year rose from 5,503 in 2006 to 67,168 in 2014: an increase of 1,121 percent.2

Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014

According to the California Attorney General, since 2012 there have been roughly 657 data breaches, affecting a total of over 49 million records of Californians, with 24 million of those records being compromised in 2015 alone.4

As the number of attacks and the number of records compromised increase, so too do the costs associated with prevention and response to cyber attacks. In 2015, the Ponemon Institute conducted an annual study of cyber-crime related costs using a sample of 252 organizations in seven countries, showing a steadily increasing trend of successful cyber attacks since 2012.5 The study also found a $2.7 million (19 percent) increase in the mean annualized value of costs for U.S. companies since 2014 (an 82 percent increase over the past 6 years), with the most expensive breaches being caused by viruses, worms, and malware.6

Public pension plans are not immune. There was a recent report of an attempted cybersecurity breach at a pension plan, wherein three separate member accounts were targeted. The perpetrators of the attack attempted to create online user accounts for three retired members using the members’ personally identifiable information (social security numbers, employer information, and addresses). It is believed that the personally identifiable information was acquired in previous breaches to other systems, where it was then placed and/or sold on the “dark web.”7 The online accounts were then used to set up direct deposit payments to an online bank. Fortunately, the breach was identified prior to any funds being dispersed. Such attacks are sure to continue as personally identifiable information becomes more readily available and commoditized in this subterranean marketplace.

Given the increase in sophistication and severity of cyber attacks, the standards upon which the targeted information is protected should be adapting in turn. Unfortunately, the technological levels for both attacks and prevention are advancing faster than the law. This creates an ongoing challenge for trustees to exercise risk oversight responsibilities and to be assured that everything that can be done is being done to protect the organization and its members’ data.
Current Standards for Cybersecurity Oversight

The Federal Information Security Management Act of 2002 (FISMA)8 provides an informative foundation for implementing a cybersecurity program. It requires each agency in the executive branch to develop, document, and implement a security program that includes:

A. Periodic assessment of risks and the scale of the harm associated with those risks;

B. Policies and procedures based on risk assessments to cost-effectively reduce risks to an acceptable level;

C. Procedures for detecting, reporting, and responding to breaches;

D. Plans and procedures to ensure continuity of operations supporting information systems;

E. Periodic testing and evaluation of the effectiveness of security policies, procedures, and practices;

F. A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the security policies, procedures, and practices; and

G. Security awareness training to inform personnel of security risks and their responsibilities in complying with agency policies.9

Since FISMA, there have been additional published standards that are currently being used by organizations to further develop their security programs, such as those published by the National Institute of Standards and Technology (NIST),10 and the International Organization for Standardization (ISO).11 There are multiple annual reports cataloging trends in types and frequencies of breaches, the types of data and organizations being targeted, as well as many other trends associated with the data.12 The cacophony of voices of doom and gloom and the catalogs of failures make it increasingly difficult to develop timely, comprehensive and effective cybersecurity policies.

The Center for Internet Security’s Critical Security Controls for Effective Cyber Defense (Controls) was created to address the challenge of synthesizing all of the information in order to prioritize cybersecurity implementations.13 The Controls are a continually updated list of procedures, based on lessons learned from actual attacks, and are designed to prevent, identify, address, and allay damage as a result of breaches.

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure configurations for Hardware and Software on Mobile Devices, Laptops Workstations and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protection
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises

Advising Trustees of Their Role in Cybersecurity Oversight (continued)
Advising Trustees of Their Role in Cybersecurity Oversight (continued)

Government regulators are also paying increasing attention to cyber risk. Recently, the Security and Exchange Commission’s (SEC) Office of Compliance Inspections and Examinations (OCIE) announced a new round of cybersecurity examinations designed to assist registered investment advisers and broker-dealers in assessing their cybersecurity programs. The initiative will focus primarily on the following six areas:

A. Governance and Risk Assessment. Inspectors may assess whether firms have cybersecurity governance and risk-assessment processes.

B. Access Rights and Controls. Inspectors may review how a firm controls access to various systems and data via management of user credentials, authentication, and authorization methods (including remote access, customer logins, passwords, and firm protocols to address customer login problems, network segmentation, and tiered access).

C. Data Loss Prevention. Inspectors may assess how a firm monitors the volume of content transferred outside of the firm by its employees or through third parties, and how the firm monitors for potentially unauthorized data transfers.

D. Vendor Management. Inspectors may focus on firm practices and controls related to vendor management. Inspectors may also assess how vendor relationships are considered as part of a firm’s ongoing risk-assessment process.

E. Training. Inspectors may focus on how training is tailored to specific job functions and designed to encourage responsible employee and vendor behavior. They may also review how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.

F. Incident Response. Inspectors may assess whether firms have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events by determining which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

Cybersecurity policies should include, at a minimum, each of the relevant CIS Critical Security Controls. Those policies should also be crafted to adequately address each of the analogous and applicable areas of oversight identified by regulatory agencies such as the SEC. Plan counsel should continually monitor pronouncements and exercises like the OCIE examinations and update policies and response plans as necessary.

Breach Litigation and Board Responsibility

Looking again to the private sector, several data breaches at US companies have raised concerns among public corporation board members as to their fiduciary responsibilities with regard to establishing a cybersecurity plan. In some cases, shareholders have filed derivative suits against the board and its directors for failing in their fiduciary duties as a result of the breach.

For example, Target Corporation’s directors and officers were sued in January 2014 as a result of the now infamous data breach of millions of Target customers’ personal financial information. In addition to claiming that the board failed to meet their fiduciary duties of due care and good faith by releasing incomplete and misleading information to customers after the breach, the suit also claimed the board failed to meet their duty of loyalty because they did not have proper security controls to detect and prevent such a data breach. The shareholder suit not only sought monetary damages for the harm to the company from the data breach and the resulting mitigation, investigation, and litigation efforts, but also injunctive relief through “significant corporate and managerial reforms to prevent future harm to the Company by disloyal directors and officers.”

In May 2014, shareholders of the Wyndham Worldwide Corporation brought a similar derivative suit after three separate data breaches that led to the theft of the personal and financial data of over 600,000 customers. The suit claimed that the board failed to ensure that the company implemented adequate cybersecurity policies and procedures prior to connecting their local computer networks to other networks. The suit against the board was ultimately dismissed. However, the court notably did not reject the theory that board members could potentially be held liable if found to have “utterly failed to implement any reporting or information system . . . [or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed.”
Despite the dismissal of the derivative suit, Wyndham Worldwide still faced charges by the Federal Trade Commission (FTC) alleging that the company unfairly placed consumers’ payment card information at risk. Ultimately, Wyndham settled with the FTC, and the language of the settlement contained provisions for the development of a “Comprehensive Information Security Program” requiring the following:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of Cardholder Data that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, (3) risks emanating from the Wyndham-branded Hotels, and (4) prevention, detection, and response to attacks, intrusions, or other systems failure;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment (including any risks emanating from the Wyndham-branded Hotels), and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.  

While there has yet to be a ruling holding individual board members responsible for information security breaches at an organization, these cases are instructive in highlighting the potential liability of trustees if the cybersecurity program within the organization is wholly non-existent or inadequate. And while Wyndham’s case with the FTC articulates what could be considered a baseline for a cybersecurity program according to the FTC, simply meeting those minimum standards will not adequately mitigate a breach due to the rapidly evolving threats organizations are facing today. However, by incorporating guidance from the Wyndham cases with NIST standards, FISMA, CIS Controls, etc., a roadmap begins to emerge for cybersecurity oversight, creating a common body of standards to be applied to a cybersecurity program with clear indications of a board’s responsibility.

The National Association of Corporate Directors (NACD), in conjunction with American International Group Inc. (AIG) and the Internet Security Alliance (ISA), has identified five steps all corporate boards should consider as they seek to enhance their oversight of cyber risks:

A. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

B. Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.

C. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

D. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

E. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

It is imperative that governing bodies and trustees provide leadership in ensuring their organizations maintain robust and up-to-date controls to detect, prevent, and respond to the increasingly sophisticated cybersecurity threat landscape. By proactively engaging and adapting to contemporary cyber threats, organizations will be better prepared to defend themselves and respond when breached. The role of legal counsel should be considered the same as in any situation posing significant
financial, reputational and legal risk for a client. Counsel should endeavor to remain informed of the changing legal and regulatory landscape, and continually track the changing risk environment. In advising plan fiduciaries, counsel should make certain that fiduciaries receive adequate information and reporting to ensure that the organization has in place robust and evolving plans for prevention, monitoring and response to cybersecurity threats and an inevitable breach.22

**Brian J. Bartow** is the General Counsel and **Braden Pate** is Counsel at the California State Teachers’ Retirement System.

### ENDNOTES

1While preparing this article, Verizon Enterprise Solutions, which releases an annual analysis on data breaches across a variety of industries, announced it suffered a breach, reportedly affecting 1.5 million business customers. Particularities on the breach have not been disclosed as of yet.


3Id. at 12.


6Id.

7The breach investigation is ongoing, and already one member targeted has acknowledged receiving previous breach notices from Anthem as well as her credit card company.

8Congress passed the Federal Information Security Modernization Act of 2014 to address the increasing sophistication of cybersecurity attacks, which reiterates the previous requirement for federal agencies under FISMA 2002 to develop, document, and implement an agency-wide information security program.

9See GAO-15-714, supra n.3 (Pages 5-6 of the GAO report detail the components set forth under FISMA 2002.).


14Id.


16Verified Shareholder Derivative Complaint, page 2, *Collier v. Steinhafel et al.*, No.14-cv-00266-PAM-JJK (D. Minn. 2014). [The litigation is currently pending as Target’s board appointed special litigation committee (SLC) determines whether, and to what extent, Target should continue to pursue the litigation.]


18Id. at 16 (quoting *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006)).


21Notably, despite the importance of this issue, a recent survey conducted by Tanium and Nasdaq found that 91% of board members admitted they cannot interpret a cybersecurity report, and nearly 40% of C-level executives, Chief Information Officers, and Chief Information Security Officers do not feel responsible for the repercussions of a breach. (*See* [Tanium/Nasdaq, *The Accountability Gap: Cybersecurity & Building a Culture of Responsibility* (2016).]