CYBER RISK OVERSIGHT FOR HIGHER EDUCATION BOARDS

Key Principles and Practical Guidance for Foundation and Institution Board Members

1133 20th Street NW, Suite 300, Washington, DC 20036

The Association of Governing Boards of Universities and Colleges (AGB) is the premier membership organization that strengthens higher education governing boards and the strategic roles they serve within their organizations. Through our vast library of resources, educational events, and consulting services, and with 100 years of experience, we empower 40,000 AGB members from more than 2,000 institutions and foundations to navigate complex issues, implement leading practices, streamline operations, and govern with confidence. AGB is the trusted resource for board members, chief executives, and key administrators on higher education governance and leadership. For more information, visit www.AGB.org.

The mission of the Internet Security Alliance (ISA) is to integrate advanced technology with economics and public policy to create a sustainably secure cyber system. ISA has three major goals: thought leadership, advocating for market-based public policy, and promoting the use of effective cybersecurity standards and practices. ISA's "Cyber Social Contract" describes an incentive based, as opposed to regulatory, approach to public policy. ISA has also partnered with AGB, NACD and other director organizations and governments around the world to develop handbooks on cyber-risk oversight that are now available on four continents in five languages. To learn more about ISA, visit www.isalliance.org.

American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange.

Printed in the United States of America.
ISBN 978-1-951635-15-2

Acknowledgments

This handbook was originally prepared by Larry Clinton, president and CEO of the Internet Security Alliance (ISA) with support from Josh Higgins, ISA's senior director of policy and communications, and further modified for the higher education governance context by AGB editors. The higher education edition was adapted from *Cyber Risk Oversight 2020* (2020) published by the National Association of Corporate Directors (NACD) In association with ISA. AGB thanks American International Group, Inc. (AIG) for its generous support in the development of this publication.

AGB, ISA, and AIG are grateful to more than 55 members and friends of AGB who added value to the resource through their comments in numerous workshops and review of the draft manuscript, which proved invaluable in strengthening the book. Special thanks to Henry Stoever, AGB President and CEO, who championed this project and whose relationship with Larry Clinton and ISA made this publication possible. We also extend our appreciation to the AGB cyber risk editorial team: Doug Goldenberg-Hart, Cristin Toutsi Grigos, Steve Pelletier, Anne Elizabeth Powell, Rachel Rosenfeld, and Merrill P. Schwartz.

AGB is also grateful for the enthusiastic and timely assistance from EDUCAUSE staff and membership in adapting the Cyber Risk Oversight Toolkit for the higher education context (with special thanks to Brian Kelly and Jarret Cummings of EDUCAUSE, and members Patty Patria and Alex Lindstrom). Finally, AGB thanks Holly Peterson, associate director of legal resources for the National Association of College & University Attorneys (NACUA) for sharing background resources on cybersecurity in higher education.

Contents

Foreword

In today's technology-driven world, it is no surprise that cybersecurity has taken on greater significance throughout our society. Every year, more news outlets report cybersecurity breaches of critical infrastructure and, financial and government systems, with severe consequences that ripple out from the affected organization and beyond. An estimated $6 trillion in global losses in 2021 from cybercrime underscore the critical importance that cybersecurity has for the global economy.

Higher education is not separate or immune from these developments. Despite critics' claims that higher education is a "slow adopter" of technology and prefers to avoid data-driven metrics, higher education institutions and foundations harness a tremendous amount of data and technology to advance their priorities. Academic and classroom data, financial information, health records, detailed research outcomes, donor information and gift agreements, delicate contract negotiations—these are but a few types of information that colleges and universities collect and produce from millions of students, faculty, staff, alumni, and donors every year. Even more so since the start of the COVID-19 pandemic and the transition to online and hybrid-education environments, institutions rely on deeply interconnected technology to carry out the fundamental components of a complicated enterprise. And unlike some corporate elements, the core functions of colleges and universities involve sharing and collaboration, including the education of students, developing research, providing a community space for the arts and science, and more. The intrinsic qualities of higher education forces leaders to provide a nuanced balance between stakeholder needs and security requisites.

It is in this context that AGB has chosen to publish *Cyber Risk Oversight for Higher Education Boards: Key Principles and Practical Guidance for Foundation and Institution Board Members*. Given both the breadth and depth of impact that cyber risk can have on institutional missions, students' success, and financial integrity, it is evident that board oversight of cyber risk is necessary to position cyber risk as part of any enterprise risk management strategy. In earlier eras, some claimed that cybersecurity was strictly an IT issue, but that kind of thinking ignores the current reality and interaction between technology and strategy.

My hope is institution and foundation board members will use this resource to understand and become inspired to learn about and proactively oversee—in collaboration with chief executives—the overarching facets of cyber risk, place this topic on future board meeting agendas, and take to heart the practical guidance, key indicators, and

proffered strategies that can ensure effective, strategic oversight. This resource's components—the five principles and the associated toolkit—were created specifically to outline exactly what higher education boards need to review and discuss with chief executives and their leadership teams in this era of constant technological innovation. While having access to cyber risk and security expertise is essential for all boards, cyber risk must also be understood by the board and relevant committees, no matter the size, location, or nonprofit status of the institution or foundation they serve. As such, this resource aims to explain and explore the topic in ways that all board members can use to contribute to robust board conversations and strategic decisions about overseeing and managing cyber risk.

I also want to express my deep appreciation for AGB's partners in creating this resource. Both the Internet Security Alliance (ISA) and the American International Group, Inc. (AIG) were instrumental in its creation, and their expertise has undoubtedly made the recommendations stronger and more relevant.

Cyberattacks are a persistent threat to colleges, universities, and institutionally related foundations. Board members have a responsibility to ask thought-provoking questions and provide relevant insights, perspectives, and suggestions based on their professional experience to strategically inform chief executives and senior staff as they advance their institutions and foundations in a world in which technology's importance will only grow in the decades to come.

Henry Stoever
President and Chief Executive Officer, AGB

Executive Summary

Cyberattacks on colleges and universities have become more frequent, more sophisticated, and more dangerous. The risks are great: successful cyberattacks can compromise an institution's reputation, result in substantial financial payouts, undermine its credit status, and foment legal challenges—to say nothing of slowing or even shutting down an institution's fundamental capacities for teaching, learning, and research. The Association of Governing Boards of Universities and Colleges (AGB) believes strongly that ensuring cybersecurity in colleges and universities requires a strong, concerted, enterprise-wide strategy at each institution. Further, AGB believes that governing boards must assume oversight for ensuring that their institution's management strategies adequately address the growing threat of cyberattacks. To that end, this handbook frames five principles that higher education governing boards need to understand in order to adequately and successfully oversee their institution's cybersecurity:

Principle 1: Board members need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.

Cybersecurity has often been relegated to the information technology department. But in higher education, maintaining cybersecurity encompasses a cascade of issues that require an enterprise-wide approach. In the context of educational institutions, cybersecurity means protecting valuable intellectual property and research; securing student, faculty, and alumni data; preserving the reputation of the institution; and ensuring that third-party vendors do not put the institution's networks and data at risk. For these reasons, cybersecurity needs to be integrated into the university or college's overall risk management strategy. This means that boards need to understand their institution's most valuable assets—their "crown jewels"—and assess what needs to be done across the entire institution to protect the institution from cyber risk.

Principle 2: Board members should understand the legal implications of cyber risks as they relate to an institution's specific circumstances.

The legal and regulatory landscape around cybersecurity in higher education is constantly evolving, including requirements for public disclosure, privacy and data protection, information sharing, and infrastructure protection. Boards need to stay informed about current compliance and liability issues faced by their institutions. Boards need to be aware of related requirements their institutions must meet, such as protocols that are driven by FERPA, HIPAA, and other federal and state cybersecurity legislation and regulations. Additionally, boards should consider including cybersecurity on board agendas

and documenting their due diligence with cyber risk oversight. Potentially, boards need to have members who are responsible for monitoring this broad area.

Principle 3: Board members should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on board meeting agendas.

Cybersecurity is now an essential element of board-level strategic decisions and needs to be integrated into discussions about issues such as reputation management, curricula development, and research. There is no single approach that will fit every board, but board members should set clear expectations with the institution's administration about the format, frequency, and level of detail of cybersecurity-related information they wish to receive. The board's approach to cybersecurity should be clearly defined in committee charters to avoid confusion or duplication of effort, and briefings on cybersecurity should occur at least quarterly. Additionally, boards should consider bringing outside expertise to evaluate the institution's cybersecurity to provide a broader perspective on the risk to the institution and progress made in mitigating any potential or existing risk.

Principle 4: Board members should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.

Institutions need to have a technical framework (or a variety of frameworks) with cybersecurity controls that address cybersecurity risk. More importantly, institutions need to have a management framework that strategically coordinates all aspects of the institution that relate to cybersecurity, including plans for business continuity should the institution's cybersecurity be breached. Board members should seek assurances that the administration is taking an appropriate enterprise-wide approach to cybersecurity and should see that such efforts are adequately funded and staffed.

Principle 5: Board-administration discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance,

CYBERSECURITY DEFINED

The term "cybersecurity" refers to measures intended to safeguard the confidentiality, integrity, and availability of information by protecting the computer systems, networks, and programs that gather, store, and transmit that information. A cybersecurity strategy may make use of several such measures in combination, depending on the type of information that requires protection, the nature of the organization responsible for protecting it, and the level of risk.[1]

as well as specific plans associated with each approach.

Without micromanaging the details, boards need to fully understand the standards, controls, and processes that management uses to determine the effectiveness of the institution's approach to reducing exposure to cyber risk to acceptable levels. The board's work in helping to quantify cyber risk management through exercises such as assessing the institution's overall appetite for risk and measuring institutional practices in the context of commonly accepted practice and guidelines helps enable the institution to make better risk-informed decisions about strategy and, in turn, better decisions about the allocation of resources.