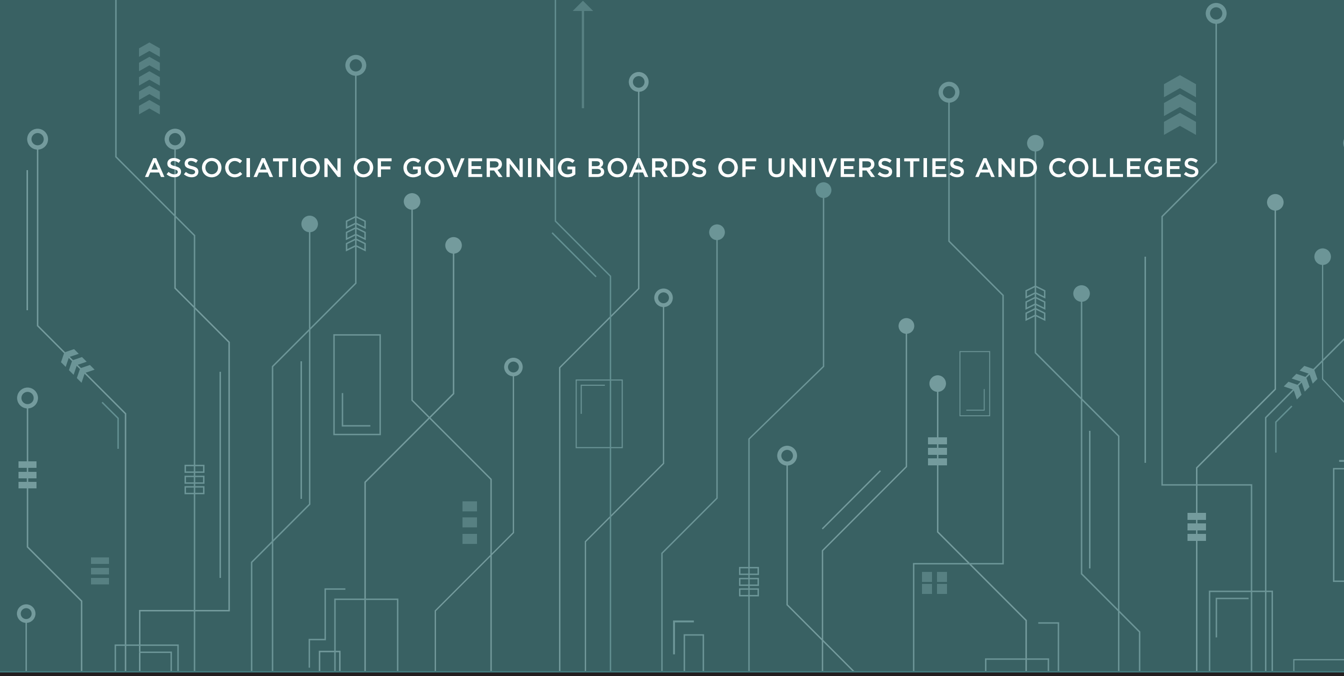

ASSOCIATION OF GOVERNING BOARDS OF UNIVERSITIES AND COLLEGES

WHAT BOARD MEMBERS NEED TO KNOW ABOUT

Cybersecurity

By Michael Hites, George Finney, and Joseph D. Barnes

AGB
PRESS

CONTENTS

WHAT CYBERSECURITY IS AND WHY IT MATTERS

While bank robbery is broadly familiar from movie depictions and news reports, most people do not think of college or university robbery. Yet, just like banks, colleges and universities around the world process hundreds of billions of dollars in loans every year. And, unlike banks, they also collect a vast array of personal information—about students, parents, faculty, and donors—and develop considerable intellectual property through research and innovation. So, although we tend not think of colleges and universities as targets of robbery, in some ways they have a lot more at stake than banks do.

To rob a bank in the 1980s, you needed a weapon, a mask, and a getaway driver. You needed to case the location and probe the bank's security: Are there cameras, security guards, or alarms? How busy is it at certain times of the day? Most important of all, you needed to know the times of day when the vault was unlocked. Even the most sophisticated plot could fall apart, and you could find yourself caught red-handed. To rob a bank today, all you need is a computer. You probably do not even need to leave the house—even if your house is in South Africa or Bangladesh, and the bank you are robbing is in Japan. And unlike your counterparts of thirty or forty years ago, you run almost no risk of ever getting caught.

Nearly every business is now located in the bad part of town on a street patrolled by vandals, vigilantes, criminals, and spies from all over the world: the internet. The internet exposes all types of business, including higher education, to an array of risks. Criminal breaches of networks and information systems can result in financial loss, identity theft and fraud, disruption of services, damage to systems, and loss of access to sensitive or essential data. Even in the good parts of town, most banks have vaults, bulletproof glass, alarms, and exploding money filled with permanent dye that can be used to track criminals. But what kinds of protections are available to guard against the risks of connecting to the internet?

Cybersecurity for Colleges and Universities

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 it. 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.

Colleges and universities are relatively complex organizations with risk exposure beyond that of many businesses. While a college or university may have an employee count equivalent to some medium to large businesses, for example, it may also function as a landlord and internet service provider for residential students. Some campuses have wireless networking with coverage areas rivaling those of nationwide hotel or retail coffee chains. And while a corporation or private company can readily impose and enforce restrictions on access to information, an institution of higher education must carefully weigh the effects of such measures on the academic freedom of students and faculty. Open access to information is widely regarded as essential to the educational enterprise and necessary to sustain academic community. As a result, colleges and universities may be inclined to take a less restrictive approach to security—an approach that can cause cybercriminals to view them as "soft targets."

Open access to information is widely regarded as essential to the educational enterprise and necessary to sustain academic community.

Cybercriminals may exploit vulnerabilities in campus networks to obtain access to credit card or Social Security numbers, or they may attempt to transfer funds directly out of an institution via fraudulent invoices or by diverting direct deposits. Nation-states may target research information or intellectual property, and "hacktivists"—those with social or political motivations for hacking computer systems—may target a college or university for what is being said or done on its campus. Increasingly, hackers are targeting the sensitive information to which campus police have access, such as arrest records and closed-circuit television footage. The presence of a major athletic stadium or large concert venue on a campus raises both the stature of the institution and its visibility to attackers.

This publication provides a basic overview of cybersecurity threats facing higher education institutions and what can be done to guard against them. It is designed specifically for members of college and university governing boards and to strengthen board capacity for effective oversight in this increasingly important area.

What Is a Cyberattack?

Most people have gained a general awareness of cybersecurity challenges from news reports of data breaches affecting high-profile companies and institutions, phishing scams through which criminals gain access to secured networks or sensitive information, and ransomware attacks in which important data are held hostage for large sums of money. The incidence of such cyberattacks is growing rapidly, and it is essential that any cybersecurity strategy account for these types of threats.

A *data breach* is an incident that puts at risk of exposure sensitive personal information such as Social Security and driver's license numbers or financial and medical records. In 2016, the number of reported data breaches nationwide increased by 40 percent over the previous year (from 780 to 1,091).[1] Approximately 3 percent of these breaches occurred in the education sector.[2] The actual number of breaches is likely far higher. Most breaches go unreported because there is no obligation to report an incident, unless the victim is a public corporation or the personal information of customers has been exposed.

Phishing is sending an email message to a large number of recipients in order to obtain personal or login information from at least some of them. The criminal who thus obtains a credit card number, for example, can make a purchase from an online retailer and have the merchandise sent to a third party. With login information, the criminal can access a college or university email account and use it to change direct deposit information. A compromised account can also be used to send spam, creating the appearance that this unsolicited email comes from a legitimate source. A college or university that fails to prevent spam originating from its email server will suffer the consequences of a damaged email reputation. Eventually, spam appliances will block email from the institution, which can affect the bottom line—decreasing applications, for example, or reducing donations.

In 2016, the number of reported data breaches nationwide increased by 40 percent over the previous year.

Spear phishing is a more refined form of attack in which a targeted message is sent to an individual or a small group. For example, the attacker may know that the president goes by Billy, not William, and create a message asking the recipient(s) to transfer funds or route a purchase request in a hurry. This type of message appears to be authentic and may be forwarded widely among faculty

RISK MANAGEMENT

It is not feasible for a college or university to operate without being connected to the internet. Therefore, the inevitable security risks must, like all other institutional risks, be managed. A *scorecard* is commonly used to evaluate the likelihood of financial or reputational impact. Given that hackers are constantly looking for flaws in the IT systems of colleges and universities, the likelihood of a breach is high—more a matter of when, not if. Accordingly, the risk score associated with digital information is also high. Assessing the anticipated impact involves assigning a dollar value to a data-theft event. What will be the cost in terms of immediate financial impact and reputational damage, and what will be the cost of assisting those whose information is stolen?

The assessment of cybersecurity risk can lead to the temptation to lock down all information completely. That is not practical, however, because locking down all data would make it considerably more difficult to operate the institution. Instead, once the top cybersecurity risks have been identified, access to data should be restricted to the greatest extent possible without causing excessive burden on the institution. There is simply no way to guarantee the safety of all data.

At many institutions, an enterprise risk management program collects and ranks all the possible risks. This allows an institution to focus on the highest risks, whether related to cybersecurity or not. A *risk register* is one of the simplest ways to identify risks to an institution's cybersecurity as well as to help prioritize the response to those risks (see appendix A). Commercial tools that automate risk monitoring are available, but because they are expensive and require significant effort to maintain, these tools are not usually a good fit for small institutions. Instead, a brief survey of IT employees and other stakeholders can be used to identify significant risks. These risks can be captured and categorized in a spreadsheet, creating a risk register that enables the institution to track progress from year to year. A risk register can also be used to align day-to-day operational security tasks with the overall security strategy.