Frequently Asked Questions

What is cyber risk? ............................................................................................................................ 3
What is cyber insurance? .................................................................................................................... 3
What are the aspects of coverage? ..................................................................................................6
What data are covered by cyber liability insurance? .................................................................... 6
What losses are not covered? ........................................................................................................... 8
Will other types of insurance cover cyber risk? ............................................................................ 8
Are there any special concerns for public institutions? ............................................................... 9
What is the process for buying cyber insurance? ......................................................................... 9
What are the tradeoffs of self-insuring rather than buying cyber liability insurance? ...........10
What are the implications of cyber insurance on an institution’s computing systems and processes? ................................................................................................................................. 11
What should happen when an event occurs that might be covered by cyber insurance? .....12
What do institutions need to know about the claim process? ..................................................12
Will an institution’s cyber liability insurance premiums rise after making a claim? ............13
This document contains advice intended for general information only. To learn how cyber insurance applies to your institution, please contact your institution’s risk management office or chief information officer. This document is not legal advice. For legal advice, please contact your legal counsel.

What is cyber risk?

Cyber risk refers to the risk of financial harm to an organization resulting from the failure or disruption of its computer systems. Alternatively, it is the risk companies face from their handling data and relying on technology in their day-to-day operations. As used by insurers, “computer systems” is typically defined broadly to include many information technology systems.

Insurers view colleges and universities, with their culture of openness and information sharing, as highly susceptible to cyber risk. Data breaches can turn into high-visibility problems, such as identity theft, electronic stalking, compromise of health data, theft of intellectual property (either the institution’s own or that of another entity), and other liabilities.* In early 2016, a well-known U.S. university disclosed that it fell victim to an attack on its financial management software in late 2015 that compromised the information of 80,000 current and former students, employees and vendors. Cyber risks at educational institutions encompass all users, including faculty, students, and staff. Colleges and universities are also a treasure trove of confidential information, with financial records of parents, health care records of students and staff, credit card data, etc.

* EDUCAUSE research indicates that data breaches at higher education institutions seems to be falling. See D. Christopher Brooks and Joanna Lyn Grama, “Searching for a Smoking Gun, Chasing a Silver Bullet: Data Breaches in Higher Education,” research bulletin (Louisville, CO: ECAR, February 21, 2017). Other research shows that the higher education reputation for being a risk environment may be somewhat undeserved. See Kim Milford and Joanna Lyn Grama, “This Magic Moment: Reflections on Cybersecurity,” EDUCAUSE Review, September 28, 2015.

What is cyber insurance?

Cyber insurance is a financial risk transfer product that helps protect organizations from cyber and information technology risks by transferring those risks away from the insured. Today, insurance coverage exists for variety of potential losses and liabilities caused by cyber risks. Insurance for particular institutions may include some or all of the following:
Breach and event response coverage: This coverage covers the following costs resulting from a privacy breach: forensic and investigative services; breach notification services (including legal fees, call center, mailing of materials, etc.); identity and fraud monitoring expenses; public relations and event management.

Regulatory coverage: The Securities and Exchange Commission, the Federal Trade Commission, the Department of Homeland Security, and dozens of other local, state, federal, and non-U.S. regulators now look at all aspects of cyber risk. This coverage reimburses the costs to defend an action by regulators due to a privacy breach, but there is no limitation as to what caused the privacy breach. Coverage would apply to a failure of security that causes a privacy breach, someone losing a laptop, or someone e-mailing a document to the wrong person. Coverage also applies to nongovernmental regulations, in particular the payment card industry and its PCI standards. It also covers any fines and penalties imposed by a court or regulator or imposed by certain nongovernmental organizations, if insurable by applicable law.

Liability coverage: Liability insurance protects the policyholder and insured individuals from the risks of liabilities imposed by lawsuits and similar claims. It protects the insured in the event he or she is sued for claims that come within the coverage of the insurance policy. Liability insurance may also cover some costs incurred by the policyholder in responding to the claim or lawsuit but not costs the policyholder incurs to fix the issue. Common types of cyber insurance liability coverages include:

- Privacy liability: This coverage covers defense and liability for failure to prevent unauthorized use/access of confidential information (including the failure of others to whom you have entrusted data). Coverage generally extends to personally identifiable information and confidential information of a third party.

- Security liability: This coverage covers defense and liability for the failure of system security to prevent or mitigate a computer attack, including but not limited to the spread of a virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use.

- Multimedia liability: This coverage covers defense and liability for media tort from online publication, including libel, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, or negligence in content. Coverage extends to the institution’s own websites, e-mail, and media activities such as blogging and tweeting. For example, if a blog contains
libelous information and claim for compensation is made against the institution, this coverage applies.

**Internal expenses and court attendance cost to defend claims:** Under a cyber insurance policy, the insurer may have the right and duty to defend any claim brought against an insured or may indemnify the insured for reasonable costs incurred by the insured to defend a claim. An insured will generally be required to cooperate with the insurer in the defense of the claim and provide to the insurer all information and assistance that the insurer reasonably requests, including attending hearings, depositions and trials and assistance in effecting settlements, securing and giving evidence, obtaining the attendance of witnesses, and conducting the defense of any claim covered by the policy.

**Cyber extortion:** Cyber extortion usually takes the form of a ransomware attack, whereby a cyber criminal will encrypt a victim’s files or threatens the release of sensitive data unless a ransom is paid. Cyber extortion coverage covers the costs of consultants and monies, including cryptocurrencies, for threats related to interrupting systems and releasing private information.

**Institution’s loss of income or extra expenses due to:**

- **Security breach:** Business interruption coverage covers the loss of income and extra expenses resulting from a business interruption due to a security event or an unintentional or unplanned outage. Typically, the insured entity must satisfy a waiting period or meeting a damage threshold before coverage will apply.

- **Security breaches of contingent third parties:** Many polices now recognize the interdependence of businesses and contain contingent business interruption provisions. Contingent business interruption coverage covers an insured’s loss of income and extra expense due to a security event that interrupts the service of an entity not owned, operated, or controlled by the insured but that is relied upon to conduct business. For example, if a ransomware attack prevents a payroll service from processing an institution’s payroll and the institution incurs costs to manually provide the payroll, the extra cost of doing so would be covered.

- **System failures:** A system failure generally means any unintentional and unplanned outage of a computer system. A system failure may occur, for example, after an organization implements a system patch that proves to be incompatible with existing functions resulting in an unplanned outage.
Data replacement costs due to a security breach: This coverage applies to the costs incurred by the insured to replace, restore, or recollect digital assets from written records or from partially or fully matching electronic data records due to their alteration, corruption, or destruction from a network operations security failure.

Deceptive fraud transfer: Deceptive fraud transfer is a type of cyber crime that occurs when a person is tricked into transferring funds to an unauthorized person or account. In these schemes, cyber criminals often hack into a company’s network to send official-looking company e-mails to induce company employees to transfer funds to a purported legitimate account. Deceptive fraud transfer schemes are sometimes called social engineering fraud.

What are the aspects of coverage?

Cyber insurance policies may include some or all of the following key components:

- Media in the control of others: Cyber insurance may cover unencrypted media in the care or control of third-party processors.

- Events occurring during policy period but discovered afterward: Coverage under a cyber insurance policy is triggered, in part, by an insured’s report of a claim to the carrier. Depending on the wording of the policy, it may cover events that occurred during the policy period but were discovered after the expiration of the policy period. Under a “claims made and reported form,” for example, a claim must be made and written notice of the claim must be received by the insurer during the policy period or, if applicable, during any extended reporting period that may extend the discovery period for a period of time beyond the expiration of the policy.

- Coverage for privacy breaches other than electronic or computer related: In addition to a breach of a computer system, personal data may be compromised when paper records are lost, stolen, or improperly handled, resulting in an unauthorized disclosure. For example, a privacy breach may occur when personal data paper records are not properly disposed.

What data are covered by cyber liability insurance?

Cyber insurance policies protect some or all of the following types of data:

Personal health information (PHI): Also referred to as protected health information, PHI is any information that contains individually identifiable health
information and generally includes any part of a patient’s medical record such as health status, provision of health care, or payment for health care. Federal law, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), sets forth various requirements regarding the handling of PHI.

**Personally identifiable information (PII):** PII is information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII generally includes an individual’s name, address, telephone number, Social Security number, account numbers, account balances, account histories, and passwords. It includes information that is subject to Family Educational Rights and Privacy Act (FERPA).

**Payment card information (PCI):** This includes the personal information held by a payment card brand to process a payment card transaction. PCI also refers more broadly to the Payment Card Industry. PCI-DSS (or the Payment Card Industry Data Security Standards) refers to the rules, regulations, standards, or guidelines adopted or required by the payment card brand or the Payment Card Industry Data Security Standards Council relating to data security and the safeguarding, disclosure, and handling of protected information.

**Confidential third-party/research information:** In many cyber insurance policies, sensitive third-party data such as trade secrets, designs, forecasts, methods, formulas, and records that are in the care, custody, or control of an insured may be considered “confidential” or “protected” information. A privacy event may occur under a cyber insurance policy when there is an unauthorized disclosure of confidential or protected third-party information. For example, if a professor’s research database containing information on the social behaviors of individuals who have AIDS is breached and the data are taken, insurance may cover the cost of claims made against the institution and the professor by those whose information is violated.

**Data hosting, outsourced electronic processing, or data storage:** Organizations often rely on third parties, such as cloud providers and data centers, to perform critical business functions. Coverage under a cyber insurance policy may extend to a computer system operated by a third party for the benefit of the insured. For example, an insurance policy may consider a third party’s computer system operated solely for the benefit of an insured as part of the “insured’s computer system.” Cyber insurance policies may also extend coverage to a “shared computer system,” which is a computer system, other than an insured’s computer system, operated for the benefit of an insured by a third party under written
contract with an insured and may include such systems as data hosting, cloud services or computing, co-location, data back-up, data storage, data processing, platforms, software, and infrastructure-as-a-service.

**What losses are not covered?**

Like other insurance policies, cyber insurance policies exclude coverage for certain losses. Exclusions are usually grouped together in a section of the policy, though coverage may also be excluded or limited by the definitions or policy language. Typical exclusions include claims attributable to or arising from war, operation of a nuclear facility, intentionally dishonest or criminal acts, breach of contract, theft of trade secrets, unfair trade practices, and employment practices. Insurance carriers exclude these risks because they are unwilling to insure these risks, because coverage may exist in another policy, or because coverage may be against public policy. Cyber insurance policies also typically exclude coverage for any incident or claim that arises from or is based on a willful, intentional, deliberate, malicious, fraudulent, dishonest, or criminal act or omission committed by the insured. The general intent of this exclusion is to prevent the insured from receiving a financial benefit for committing an unlawful or dishonest act.

**Will other types of insurance cover cyber risk?**

Common institutional insurance policies such as general liability, directors and officers, property may provide limited coverage. Insurance coverage for cyber risks has evolved over time. Before there was specific privacy and data security coverage, organizations may have turned to their general liability, errors and omissions, or crime policies for coverage. In some instances, these more traditional policies provided the necessary coverage, but in other cases they did not or were very limited in coverage, leading to a more tailored product designed specifically to mitigate cyber risks. For example, under a commercial general liability policy, electronic data are generally not considered tangible property and are not covered under the property damage provisions. A modern cyber insurance policy, however, may cover the costs incurred to replace, restore, or recollect digital assets from written records. Should multiple insurance policies cover the same claim, the order in which insurance policies will respond is determined by the “other insurance” provisions in the policy.
Are there any special concerns for public institutions?

The legal doctrine of sovereign immunity protects some governmental entities, including some public educational institutions, from being sued. State legislatures, however, have passed laws waiving immunity for certain actions, defining limits for the immunity provisions, and setting forth procedures to bring a claim. For example, although suit may be brought against a public entity, the law may prohibit punitive damages or place a cap on a monetary award. This may mean that, in some situations, private individuals may not be able to sue a state or public institution for a data breach or may be required to follow certain procedures in order to sue a public institution for a data breach.

What is the process for buying cyber insurance?

Like organizations in other industries, institutions of higher education face cyber risk exposure. On average, higher education institutions warehouse volumes of sensitive data and are also susceptible to losses related to business interruptions. Since not all cyber risk can be minimized through robust processes or technical controls, risk transfer is a viable means of limiting the scope of an educational institution’s exposure.

While there is no outright federal or state law mandating that higher education institutions carry cyber insurance, state or university officials may nevertheless determine that carrying such coverage is in the best interests of the university. The EDUCAUSE Core Data Service shows that, as of 2016, 51% of responding institutions have fully integrated the purchase of cyber liability insurance into their information security programs. Benchmarking the purchase of cyber insurance typically is based on comparisons with organizations of a similar industry and revenue size. Insurance brokers may have benchmarking information based on client data. Other sources are through surveys of peer institutions.

Best practices for obtaining a cyber liability insurance quote include the following:

**Work with an experienced broker:** An effective broker should have a strong, comprehensive grasp of the scope of an organization’s cyber risk; understand and explain how this risk is quantified; provide recommendations on insurance carriers or policies that might be a good fit for the organization; and obtain appropriate coverage and favorable pricing. Selecting a broker with cyber insurance expertise may be essential to securing cyber insurance that addresses the institution’s needs. Because insurance companies use policy forms for all
kinds of organizations, colleges and universities should review policy language to look for terms and provisions that are unclear in the higher education context and address these prior to purchasing the policy.

**Conduct a security risk assessment to reduce premium:** A risk assessment provides greater transparency into the organization’s cyber security controls and helps the organization identify vulnerabilities and potentially make changes to areas in need of improvement, which, if properly implemented, could result in a premium reduction. The EDUCAUSE Core Data Service reports that, as of 2016, 14% of responding institutions have conducted an information security risk assessment for insurance purposes.

**Implement security controls that reduce premium:** Cohesive and interconnected corporate practices geared around people, process, and technology-related cyber security improvements reduce risk and can lead to lower premiums. Restricting network access to certain users is an example of a solution that impacts all three categories: a corporate policy mandates the network access restriction; the restriction is executed by an information security or information technology team; and one of the policy’s core objectives is to limit human error.

**What are the tradeoffs of self-insuring rather than buying cyber liability insurance?**

Organizations, working with an experienced insurance broker and risk management professionals, must evaluate their own cyber risk appetite and what steps they intend to take to mitigate those risks. Cyber insurance is not a “fix all” for all risk mitigation policies and procedures, and it has limitations. For example, it is not intended to cover the theft of money/funds (this is what a dedicated crime policy does). Cyber insurance also generally does not cover the impact on institutional reputation, the devaluation of a trade name, or the loss of intellectual property. The administrative burden to deal with the incident or prosecute an insurance claim is also not covered. The cyber insurance market can be volatile. Generally speaking, purchasing cyber insurance requires more effort in responding to the insurer’s need for information than buying other kinds of insurance, and there is still a dearth of data other than that related to PII-related breaches.
What are the implications of cyber insurance on an institution’s computing systems and processes?

Cyber insurance is a companion piece or safety net that sits alongside and complements organizational cyber security controls. It is not intended to substitute for technical, process, or human-related cyber security (e.g., ongoing training and awareness of end users of cyber security protocols). That said, if organizational computing systems or processes are victimized or otherwise fail to prevent a cyber attack, cyber insurance helps minimize the resulting financial impact.

Key organizational cyber security stakeholders (the CISO, CIO, CPO, CFO, GC, CRO) should be fully engaged in all cyber insurance–related purchase discussions, given that—similar to discussions about predictive analytics and other quantification or comparative tools provided by insurance brokers, carriers, or outside consultants—these stakeholders are best positioned to understand the scope of their organization’s cyber risk and provide recommendations on how much risk transfer may accordingly be necessary.

Other implications of purchasing a cyber liability insurance policy include the following:

**Improved cyber security through pre-breacht services**: Many cyber insurance policies include free or discounted services that can be used by policyholders before a breach occurs in order to reduce the likelihood or severity of a future cyber incident. These services can include online security assessments, access to cyber security expertise through consulting services or white papers, and cyber security awareness training programs for users. Many insurers also maintain lists of preapproved vendors or third-party partners who provide discounted services, such as incident response planning, tabletop exercises, and compliance assessments. Using pre-breacht services that are included as part of a cyber insurance policy can be a cost-effective way for an institution to improve its cyber security posture.

**Assistance to institution in making security decisions**: Some insurance brokers and carriers have in-house personnel who provide security enhancement recommendations on matters such as third-party vendor exposure, measuring organizational compliance with voluntary frameworks such as NIST and ISO, and gauging the potential financial impact of business interruption losses.
Adding cyber insurance to insurance requirement imposed on contract partners: For organizations with an extensive supply chain or reliance on third-party vendors, requiring cyber insurance may be highly advisable. Higher education institutions might add cyber insurance to contracts with partners or might find that contract partners increasingly require that the institution maintain cyber insurance.

Insurer requirements to encrypt portable media/computing devices: Insurers do not necessarily require encryption of data “at rest” or in process, but organizations that can demonstrate this capacity to insurers either on an insurance application or during the underwriting process may lead the insurers to consider the institution less risky, which may result in a premium discount.

What should happen when an event occurs that might be covered by cyber insurance?

In the immediate aftermath of a cyber event, an organization with cyber insurance should immediately notify its insurer and broker. Prompt notification is preferred but in any event should not occur beyond the requirements specified in the insurance policy. Prompt reporting is highly recommended even if the organization—for any of a number of reasons—decides not to file a claim.

Many insurers have a counsel panel and other preapproved vendors that the organization can utilize in the aftermath of a breach for remedial, legal, and other costs. To avoid delays and maximize organizational operability, it is highly recommended that the organization have a preexisting relationship with each vendor or at least have some measure of familiarity with them prior to a breach. If an organization wants to use a vendor that is not on an insurer’s counsel or preapproved vendor list, this usually is not a problem so long as the insurer is made aware prior to an incident.*

* EDUCAUSE maintains a number of resources to assist institutions in responding to an information security incident. See the Incident Response and Management Toolkit.

What do institutions need to know about the claim process?

Typically three parties are involved in the claims handling process: the insured organization’s defense counsel, broker claims assistance, and the insurer’s claims team. During the claims process, the organization’s insurance broker provides related assistance and advocacy and also assists with settlement strategies and
responding to coverage questions. Generally speaking, a major factor for organizations when deciding between insurers is claims-paying history.

A benefit of cyber insurance is access to people who are knowledgeable about the various laws related to cyber events. Inadvertent mishandling of an event by the institution usually will not void insurance, but best practices dictate engaging the insurance company in the process of addressing the event that led to the potential claim.

Following an event leading to a claim, the institution and insurance company will evaluate what went wrong and consider alternatives to mitigate the risk in the future. The insurance company may urge certain strategies, but its ability to mandate is a function of its willingness to continue as the insurer and whether the market provides the insurer leverage.

In some instances, a breach may occur in a country or jurisdiction without legal requirements to notify—in such cases, the institution may want to act out of a sense of doing what is right or to reduce potential liability even though the institution has no legal requirement to act. The cost of these actions may be covered by insurance even though not legally required.

Will an institution’s cyber liability insurance premiums rise after making a claim?

Insurers tend to raise premiums following a loss, but the ability to do so depends on market conditions. Involving the insurance broker can help explain the steps taken to remediate the risk and emphasize the positive qualities of the institution.
Acknowledgments

This resource was created as a collaborative effort between members of the University Risk Management and Insurance Association (URMIA) and EDUCAUSE. We hope that this resource will be useful to you as your higher education institution considers cyber liability risk insurance. The following individuals participated in the working group that wrote this publication:

- Rick AmRhein, Chief Information Officer, Valparaiso University
- Todd Beekley, Senior Associate Director of Enterprise Risk Management, University of Cincinnati
- Brian Kelly, Chief Information Security Officer, Quinnipiac University
- Blake Lovvorn, Assistant Director Risk Management, University of Central Florida
- Robert Parisi, Managing Director and Cyber Product Leader, Marsh
- Andy Weisskopf, Information Security Officer, Binghamton University
- Lisa Zimmaro, Associate Vice President, Risk Management & Treasury, Temple University
- Joanna Grama, Director of Cybersecurity and IT GRC Programs, EDUCAUSE
- Glenn Klinksiek, Resource and Education Manager, URMIA

The working group especially thanks Robert Parisi for his contributions of the technical description of cyber insurance.
About the University Risk Management and Insurance Association
The University Risk Management and Insurance Association (URMIA) is an international nonprofit educational association serving colleges and universities. Our core purpose is to promote the advancement and application of effective risk management principles and practices in institutions of higher education. Our membership includes thousands of professionals at more than 600 institutions of higher education and 100 companies supporting those institutions.

About EDUCAUSE
EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision making at every level within higher education. A global nonprofit organization, EDUCAUSE members include U.S. and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 85,000 individual participants located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation.

About the EDUCAUSE Cybersecurity Program
The EDUCAUSE Cybersecurity Program offers a number of resources to help colleges and universities develop and mature their information security and privacy programs.

© 2017 EDUCAUSE. Creative Commons BY-NC-SA 4.0.