Higher Education

Effective cyber breach protection for higher education.

Essentially, a cyber breach is not a question of "if". The only question is "when?"

Information exposures within colleges and universities have many causes and are difficult to control. And even with the best systems, controls, personnel and procedures, no college or university is immune to the risk. It only takes one small human error, or an office break-in, or a clever hacker, to compromise millions of records and create potential havoc within your organisation.

Significant exposure

Colleges and universities face complex issues when a breach occurs. You maintain personal data on applicants, students, faculty and other employees, donors, trustees and board members.

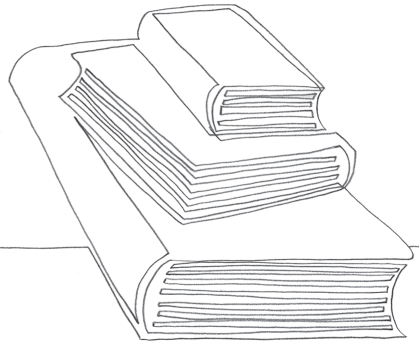
The negative publicity resulting from a data breach can lead to massive reputational and brand damage. In fact, 62% of consumers said breach notification decreased trust and confidence in the organisation.

Source: Pass or fail? Data privacy and cybersecurity in higher education

66.3m

personal records compromised between 2005 and 2018 were entrusted to educational institutions

Source: www.privacyrights.org



Regulatory landscape

The European General Data Protection Regulation (GDPR) is one of several recent global, legal and regulatory developments that impose significant new data privacy compliance and reporting obligations on organisations that manage personal data.

The GDPR introduced mandatory data breach notification obligations and expanded the regulators' authority and control, including the ability to levy significant fines. The GDPR also opens up the potential for class action style privacy claims throughout Europe, not just for financial losses but also for mental distress. Countries such as Australia, Brazil, Israel, Mexico, the Philippines, South Africa and South Korea are following Europe's lead and are implementing data privacy laws that are more robust.

These new laws and regulations present complex challenges to organisations in terms of what measures they need to implement in order to protect information over which they have custody. Responding effectively to incidents that affect this data and mitigating the potential costs and impacts of the incident is now a critical concern.

Why Beazley

Beazley, a leading insurer of technology and information security risks, has developed Beazley Breach Response (BBR), a solution to privacy breaches and information security exposures tailored to the needs of higher education.

BBR is a complete privacy breach response management and information security insurance solution, which includes a range of services designed to help you respond to an actual or suspected cyber breach incident effectively, efficiently, and in compliance with the law.

Numerous colleges and universities have turned to Beazley to help coordinate their response to data breaches.

Coverage

Breach response
- Legal services
- Computer forensic services
- Notification services for up to five million affected individuals
- Call centre services
- Credit monitoring, identity monitoring or other personal fraud or loss prevention solutions
- Public relations and crisis management expenses
- All of the policy's multiple limits will be available for breach response.

First-party
- Business interruption loss from security breach or system failure
- Dependent business interruption loss from security breach or system failure
- Cyber extortion loss
- Data recovery loss
- Data and network liability.

Third-party
- Third-party information security and privacy coverage up to £15 million
- Full media liability
- Regulatory defence and penalties
- Payment card liability and costs.

eCrime
- Fraudulent instruction
- Funds transfer
- Telephone fraud.

Criminal reward

Cyber breaches take many forms. External hackers and malicious insiders cause many breaches, but did you know that simple carelessness is responsible for a surprisingly large number of breaches?

Every breach is different. It is important to work with a partner who has been there before.

BBR Services

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage cyber breaches successfully. In each case BBR Services collaborates with you to establish the best response that is tailored to your individual needs.

BBR Services is a dedicated team of data breach professionals who assist BBR policyholders at every stage of incident investigation and breach response.

They coordinate the carefully vetted forensics experts and specialised lawyers to help you establish what's been compromised; assess your responsibility; and notify those you have to.

In addition, BBR Services coordinates credit or identity monitoring for your customers and offers PR advice to help you safeguard your reputation.

BBR Services also provides a full range of resources to help mitigate risks before an incident occurs. On our Beazley owned and managed risk management portal, beazleybreachsolutions.com, you will find resources for incident response planning, employee training, compliance, and security best practices. Newsletters and expert webinars educate you about the latest threats, preventive steps, and regulatory developments. BBR Services also coordinates a variety of pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops, so you can improve the robustness of your cybersecurity.

Case studies

Unintended disclosure

- A university sent a mailing to nearly 19,000 students regarding university clinic services and inadvertently included Social Security numbers on the address labels. The university was required to notify the affected students. BBR Services arranged all necessary breach response services including legal counsel, notification and a call centre vendor and credit monitoring.

Hacking and malware

- A university employee's computer became infected with malware, and the computer contained protected health information (PHI) and personally identifiable information (PII). Before BBR Services was notified by the university, forensic evidence was wiped in a routine clean-up by IT. The university also retained an off-panel forensics firm which concluded that no information was compromised. The university decided to get a second opinion, and BBR Services arranged for a forensics firm to investigate. The panel forensics firm reviewed documents and salvageable data, and with the help of panel counsel, determined the need to notify and offer credit monitoring to 12,000 individuals.
- A university discovered indicators of unauthorised access to an administrative unit server. Internal review suggested that as many as 400,000 students and employees had their information, including Social Security numbers, compromised. The university promptly notified BBR Services, who connected the university with forensic assistance and counsel. After the forensic investigation, and with legal support, the university was able to conclude that there was no breach as no access to the server had occurred. Thus, the university avoided notifying 400,000 students and employees.

Case studies

- A university discovered a web server was infected with malware. BBR Services immediately connected the university with counsel and a forensic firm. The forensic investigation determined the information compromised included names and Social Security numbers of 40,000 individuals, including students, faculty, applicants, alumni and employees. Forensics also determined the malware compromised names and student identification numbers of over 19,000 additional persons. The university offered credit monitoring to the 40,000 individuals whose Social Security numbers were exposed.
- A university reported a potential loss after identifying a large phishing event which involved the attackers sending large amounts of spam from a limited set of employees' outlook web access (OWA) accounts. Almost all of the emails sent looked like spam, but one of the inboxes used for the spam campaign contained a sizeable amount of sensitive information which was identified by the identity finder tool. The university contacted BBR Services and both forensics and legal counsel were retained to help respond to the matter. Fortunately, after a forensic investigation, counsel was able to conclude that there was a low probability of a breach and drafted a memorandum.

Insider

- A university learned that one of its financial aid officers was improperly removing current and prospective students' PII from computers and hard copy files, likely with the intent to sell or commit fraud. BBR Services connected the university with counsel and a forensic firm, to investigate the scope of the incident and determine which individuals needed to be notified. Counsel worked closely with law enforcement during the investigation.

"Beazley's Breach Response Services team was simply responsive, knowledgeable, and experienced. We made contact on a late Friday night and by the next morning had breach response services of legal counsel, forensics, and claims all working in parallel to mitigate and recover from our cyber event. We are grateful for the team response and expertise to work with us through the shock of the event, the magnitude of details, and the continued recovery."

Bernie Brandenburg, Risk Management Coordinator
Mercy Iowa City

beazley