# Computer Security Incidents:

## The Increased Threat and Implications for Higher Education

| *Christopher T. Davidson, MS, and Malcolm W. Beckett, DBA, MS, CISSP, Virginia Tech*

*Abstract: Computer security incidents have increased over the past decade for both the public and private sectors, and institutions of higher education are not immune to these incidents. This article explores computer security incidents and threats for higher education campuses, discusses the implications for higher education institutions, and makes recommendations for steps that higher education officials can take to mitigate these threats and incidents.*

### Introduction

The number of public reported data breaches has risen during the past decade. These incidents have included virtually every industry, and higher education has been no exception. Educause demonstrates this trend with an estimated 727 higher education breaches from 2005 to 2014, with an average of 27,509 records compromised per breach.[1] In February 2015, health insurance company Anthem, Inc. announced that online attackers breached the company's information technology (IT) system and potentially obtained "the names, dates of birth, Social Security numbers, health care identification numbers, home addresses, email addresses, employment information, including income data" of 80 million customers and employees.[2] In 2012 the South Carolina Department of Revenue experienced the theft of 3.8 million Social Security numbers, 387,000 credit and debit card numbers, information for 1.9 million dependents, and 700,000 businesses.[3] Unfortunately, computer security incidents have become more prevalent over the last decade targeting businesses, the U.S. and state governments, and institutions of higher education (IHE). In 2014 the University of Maryland experienced a similar data breach affecting approximately 300,000 records.[4] Other universities experiencing data breaches in 2014 include North Dakota University, Butler University, Indiana University, and Iowa State University.[5] These types of attacks in the private and public sectors, including colleges and universities, have the potential to cost the entity millions of dollars to provide victims with credit monitoring and to repair IT infrastructure, open the door for litigation, and harm the institution's reputation.[6] For higher education administrators, it is important that IT professionals and risk managers work collaboratively to reduce the risk of financial and reputational loss by strategically aligning both facets to the mission and vision of the organization. The purpose of this article is to discuss how computer security incidents have taken place at institutions of higher education, to discuss the implications for computer security incidents and threats for college and university administrators, to make recommendations for how IT professionals and administrators can mitigate risks from computer security incidents, and how to recover from cyber incidents.

**Colleges and universities are prime targets for sophisticated computer security incidents and threats because of the open and robust centers of information they house.**

### Computer Security Incidents and Threats on College and University Campuses

Colleges and universities are prime targets for sophisticated computer security incidents and threats because of the open and robust centers of information they house, including valuable personal information on students, faculty, and staff.[7] This personal information includes Social Security numbers, tax information, student and parent loan information, and a variety of other critical information.[8] Universities also hold intellectual property and research that could be valuable to hackers.[9] It is important to note that an institution of higher education can serve as one source of significant forms of sensitive data including personally identifiable information (PII), Health Insurance Portability and Accountability Act

(HIPAA) data, Criminal Justice Information System (CJIS) information, and restricted research. IHEs can experience as many as 100,000 or more attacks a day against campus networks primarily originating from around the world through anonymous proxy servers and other mechanisms to obscure the attacker's identity.[10]

Beyond the attempts to obtain data illegally, there are also a number of cases in which communication or media tools are defaced, including Twitter accounts like that of the U.S. Central Command and corporate and governmental websites and systems.[11] The University of Washington experienced an attack from an extremist group that took over and defaced several of the university's websites by posting text that called for the deaths of Americans in Iraq.[12] These attacks show vulnerabilities that college and university administrators must address with the use of social media and digital media.

While computer security incidents from outside sources remain an ever-growing risk for higher education administrators, human error is also a source of computer security incidents that can ultimately lead to breaches exposing an IHE to significant risk. This human error takes the form of storing PII, such as Social Security numbers, on an unencrypted mobile device that is lost or stolen. Multiple institutions of higher education have experienced these incidents and have had to provide free credit monitoring to those affected.[13] These computer security incidents have significant implications for college and university administrators.

## Implications of Computer Security Incidents for College and University Administrators

### *Financial Implications*

The most significant implication of a computer security incident and data breaches for college and university administrators are financial. In the U.S., the average cost per record for a data breach is $201. In a highly regulated field like education, the average cost per record is $294.[14] These costs can add up to hundreds of thousands of dollars or more depending on the size of the data breach. These costs can include, but are not limited to, the staff time used to address the issues through call centers, notifying victims, providing free credit monitoring services to victims, investigating the attack, and repairing infrastructure and software.[15] These costs for data breaches are not typically budgeted by college and university administrators leading officials to have to make decisions about where the money will come from to meet the institution's data breach insurance deductible or fully fund recovery activities.[16]

### *Reputational Implications*

Data breaches at IHEs cost more than the money required to address computer security incident and data breaches. There are also reputational costs for colleges and universities. This can include having to explain and apologize for an incident to students, parents, alumni, employees, trustees, and prospective students. Since colleges and universities are constantly battling for prestige and students, administrators want the reputation of the institution to focus on being a top research university, having NCAA championships, or having top faculty experts. Colleges and universities do not want to have a reputation for being the school with data breaches. While corporations are able to quantify the loss of reputation based on a decrease in revenue after a computer security incident and data breaches, the amount of reputational cost to an IHE is harder to quantify because typically students do not leave or refuse to attend a college or university based on a history of data breaches at that institution.[17]

### *Legal Implications*

One example of the legal risks caused by a computer security incident is the class-action lawsuit worth $6 billion against Maricopa Community College District (MCCD) in Arizona for a 2013 data breach that affected 2.4 million records.[18] In this case, the plaintiffs charged that the Federal Bureau of Investigation (FBI) was notified that MCCD's databases containing PII were posted online for sale in April of 2013 and that the community college district did not notify victims until November of 2013. The lawsuit alleges that MCCD knew of its vulnerabilities and failed to take the appropriate steps to address those vulnerabilities. The lawsuit also alleges that MCCD did not notify the victims in a timely manner and instead destroyed evidence of what information was actually taken from MCCD's systems.[19] If this class action lawsuit is successful, MMCD could spend another $6 billion on top of the $17 million it has

already spent to rectify this incident. While computer security incidents can reach into the millions of dollars in infrastructure, reputational, and legal costs, there are steps that college and university administrators can take to mitigate against these types of incidents.

## Recommendations for College and University Administrators

The recent data breaches in the private sector and at colleges and universities should compel university officials to examine their IT infrastructure to mitigate against computer security incidents, data breaches, and the potential financial and legal liabilities and reputational costs.[20] College and university administrators can prevent and protect against computer security incidents by completing a holistic IT risk assessment, using mobile device management (MDM), requiring multi-factor authentication for access to university databases, and carrying data breach insurance.

### *Risk Assessment*

College and university administrators should collaborate with IT professionals to complete a comprehensive risk assessment using the framework provided by National Institute of Standards and Technology under the U.S. Department of Commerce that includes risk framing, risk assessment, risk response, and risk monitoring.[21] During "risk framing," administrators and IT professionals work to produce a risk management strategy to identify, prioritize, respond to, and monitor risks.[22] During "risk assessment," administrators and IT professionals identify, prioritize, and estimate risks to the institution's operations, assets, individuals, and other organizations potentially affected by a security or data breach.[23] During the "responding to risk" stage, administrators and IT professionals identify, evaluate, choose, and implement the appropriate course of action to "accept, avoid, mitigate, share, or transfer risk."[24] During the "monitoring risk" stage, the final stage, administrators and IT professionals verify that there is compliance with the decisions and actions made to mitigate the risks, evaluate the effectiveness of those measures, and identify changes to the IT environment after measures have been implemented.[25]

**Recent data breaches in the private sector and at colleges and universities should compel university officials to examine their IT infrastructure to mitigate against computer security incidents.**

### *Mobile Device Management*

Since the work that college and university administrators has become more mobile, another area where college and university administrators can prepare to mitigate risks is by implementing mobile device management for university business such as smartphones, tablets, and laptops.[26] To address the increased use of these devices, college and university administrators need to ensure that the data on the devices are secure as a loss or stolen device could create financial and legal risks for the university.[27] With MDM, administrators can fully encrypt mobile devices with password policies and wipe devices remotely in the event of a loss or theft.[28]

### *Multi-Factor Authentication*

Another way that college and university administrators may be able to mitigate IT vulnerabilities is to use multi-factor authentication to access campus networks and databases.[29] Multi-factor authentication ensures that a user is who he or she claims to be when accessing campus networks and databases by requiring them to identify themselves using a combination of something the user knows such as: (a) user I.D. and password or PIN and (b) something like a security token that generates a one-time password (OTP). The IHE issues the user I.D. and password or PIN. The security token can be a small electronic device that the user physically possesses and generates a different OTP each time the power button on the device is pressed. There are also alternative methods for obtaining an OTP without the security token. These methods can include answering challenge questions online or having an OTP sent via message to a mobile device.[30] On college campuses, financial aid administrators are already using these devices

to log into the various U.S. Department of Education financial aid databases as mandated by the federal government to protect federal financial aid systems.[31] These devices could provide another layer of protection against potential exploitation of college and university databases by mirroring what the federal government's security procedures.

### *Data Breach Insurance*

Data breach insurance is a relatively new concept; however, it is expected to grow tremendously as current general liability insurance policies that cover injury and property damage do not cover computer security incidents and risks. Therefore, it is important for college and university administrators to invest in data breach insurance. The primary difference administrators will experience with these policies is that it lacks actuarial data. Insurers will rely on the college and university's risk management program to customize a policy to cover the college or university. The college or university's operations will dictate the coverage needed and the financial cost. Data breach policies may include liability for security or privacy breaches, costs associated with data breaches like providing credit monitoring and notifications, costs of recovering from the data breach, costs related to reputational damage, and coverage for expenses related to regulatory compliance.[32]

**General liability insurance policies that cover injury and property damage do not usually cover computer security incidents and risks.**

For administrators seeking coverage as a means for the institution to both transfer and mitigate direct financial implications, buyers will encounter both first- and third-party insurance coverage from insurers. First-party coverage includes losses to the university's own data, lost income, or other harm to the university resulting from a data breach. Third-party coverage includes insurance against liability of the university to third parties, like students and employees, resulting from a data breach.[33]

#### *First-Party Coverage*

Types of first-party coverage may include (a) theft and fraud, (b) forensic investigation, (c) business interruption, (d) computer data loss restoration. Theft and fraud coverage includes the destruction or loss of the university's data due to a computer security incident. A forensic investigation, which is almost always warranted and often required due to regulatory requirements, covers the legal, technical, and related costs due to the exhaustive and labor-intensive investigation that may require manually analyzing logs and network traffic. Business interruption coverage covers lost income and other costs related to the college's inability to conduct business because of a data breach. Coverage for computer data loss restoration includes the physical damage to or loss of computer-related assets. These assets include retrieving or restoring data, hardware, software, or other information destroyed during a computer-security incident.[34]

#### *Third-Party Coverage*

Types of third-party coverage may include (a) litigation and regulations, (b) regulatory response, (c) notification costs, (d) crisis management and public relations, (e) credit monitoring, (f) media liability, (g) privacy liability. Coverage for litigation and regulations covers costs from civil lawsuits, settlements, and fines for incidents. Regulatory response coverage covers the legal, technical, and forensic services needed to respond to governmental inquiries, investigations, fines, and other actions taken against the university. Notification coverage reimburses the costs to notify students, employees, and other stakeholders affected by computer security incidents. Crisis management coverage includes the management and public relations costs relating to educating those affected. Credit monitoring coverage covers the cost of credit and fraud monitoring to those affected by a computer security incident. Privacy liability coverage protects against the liability to employees for a breach of privacy.

#### *Recommendations for Purchasing Insurance Coverage*

Before administrators purchase data breach insurance coverage, they should identify what their unique risks are and understand what the institution's current coverage includes. This process involves getting stakeholders

involved to assist with obtaining the right types of coverage. Once this evaluation is complete, then the administrator should purchase the most appropriate coverage for the university with the appropriate limits. When purchasing insurance, administrators should be aware of any exclusions from their coverage including acts by third-party vendors. Lastly, administrators should be completely aware of what activities trigger coverage under their policy.[35]

It is important to note here that regardless of the insurance coverage, it is impossible to mitigate the social cost and damage to the reputational damage caused by a data breach.

## Conclusion

The last decade-and-a-half has seen an increase in computer security incidents and data breaches on college and university campuses. These attacks and breaches range from direct attacks from foreign and domestic hackers looking to exploit PII and research to human errors including the loss or theft of laptops that store PII. College and university administrators must work with IT professionals and college risk managers to identify and mitigate vulnerabilities in campus IT systems and infrastructure. Failing to identify and mitigate IT vulnerabilities may result in large amounts of personal records stolen, significant financial costs in the millions of dollars for colleges and universities, and a loss of institutional reputation and trust among all campus constituents.

## About the Authors

*Dr. Malcolm W. Beckett* currently serves as the director of information technology for administrative services at Virginia Polytechnic Institute and State University. In this role, he leads the organization and technical resources supporting the division's technology needs. Dr. Beckett has a background in public service where he has worked at all levels of government, including service as a first responder. In these roles, he has led numerous cross-functional and inter-disciplinary teams where he balanced the strategic needs, operational requirements, and limitations. Much of his work has concentrated on utilizing technology to supplement and enhance business processes while providing stakeholders the tools necessary to succeed. Dr. Beckett holds a Doctorate of business administration from the National Graduate School of Quality Management, a Master of Science from Capitol College, and a Bachelor of Science from Bluefield College. In addition he holds several professional certifications including the Certified Information Systems Security Professional (CISSP) Project Management Professional (PMP) certification. He is a member of Association for Continuing Higher Education (ACHE), Institute of Electrical and Electronics Engineers (IEEE), and the American Society for Quality (ASQ).

*Chris Davidson* is a doctoral student in Virginia Tech's higher education program and a graduate assistant at the Virginia Tech Institute for Policy and Governance. His research interests include emergency and crisis management, Title IX of the Education Amendments of 1972, and due process, governance, leadership, and policy in higher education. He holds a B.S. in history and social sciences and a M.S. in counseling and human development from Radford University.

### Endnotes


1 Educause Center for Analysis and Research, "Just in Time Research: Data Breaches in Higher Education," (2014), https://net.educause.edu/ir/library/pdf/ECP1402.pdf.

2 Anthem, "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services," (2015), http://www.anthemfacts.com.

3 Brown, Robbie, "South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere," *The New York Times*, (November 12, 2012), http://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html?_r=0 .

4 University of Maryland, "UMD Data Breach," (2014), http://www.umd.edu/datasecurity/.

5 Robin Hattersley Gray, "Top 10 Data Breaches at Educational Facilities in 2014," *Campus Safety Magazine*, (January 19, 2015), http://www.campussafetymagazine.com/article/top_10_data_breaches_at_educational_facilities_in_2014/Data_Breaches .

6 Blustain, Harvey, Janice M. Abraham, Rebecca L. Adair, Elisabeth J. Carmichael, Glenn Klinsiek, and Jane W. Thompson, "Risk Management," in *College & University Business Administration* (Washington DC: National Association of College and University Business Officers).

7 Pérez-Peña, Richard, "Universities Face a Rising Barrage of Cyberattacks," The New York Times, (July 16, 2013), http://www.nytimes.com/2013/07/17/

education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all .

[8] McDonald, Ryan, "Why the University of Maryland was ripe for a cyber attack," Baltimore Business Journal, (February 20, 2014), http://www.bizjournals.com/baltimore/blog/cyberbizblog/2014/02/why-the-university-of-maryland-was.html .

[9] Ibid.

[10] Zalaznick, Matt, "Cyberattacks on the rise in higher education," *University Business*, (2013), http://www.universitybusiness.com/article/cyberattacks-rise-higher-education.

[11] Barnes, Julian E. and Danny Yadron, "U.S. Probes Hacking of Military Twitter Accounts by Pro-Islamic State Group," *Wall Street Journal* (January 12, 2015), http://www.wsj.com/articles/u-s-investigating-apparent-hack-of-military-twitter-account-by-islamic-militants-supporters-1421086712 .

[12] Cihon, Brett, "Some University of Washington websites hacked; extremist group claims responsibility," (January 29, 2015), http://q13fox.com/2015/01/29/some-university-of-washington-websites-hacked-extremist-group-claims-responsibility/ .

[13] McCarthy, Kyle, "5 Colleges with Data Preaches Larger Than Sony's in 2014," *The Huffington Post*, (January 15, 2015), http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html.

[14] Ponemon Institute, "What does a data breach cost?" (2015), http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach-risk-calculator-infographic/index.html .

[15] O'Neil, Megan, "Data Breaches Put a Dent in College's Finances as Well as Reputations," *The Chronicle of Higher Education*, (March 17, 2014), http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/.

[16] Ibid.

[17] Ibid.

[18] "G&K Attorneys File Class-Action Lawsuit Against Maricopa County Community College District for 2013 Security Breach," (2015), http://www.gknet.com/news/press-release/gk-attorneys-file-class-action-lawsuite-maricopa-county-community-college-district-2013-security-breach/ .

[19] Ibid.

[20] O'Neil, Megan, "Data Breaches."

[21] US Department of Education, "National Institute of Standards and Technology, Managing Information Security Risk: Organization, Mission, and Information System View," (2011), http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf., 32.

[22] Ibid. 33

[23] Ibid., 37.

[24] Ibid., 41.

[25] Ibid., 45.

[26] Schwartz, Karen D., "How to Save Money, Time and Sanity with Mobile Device Management Software," *Ed Tech*, http://www.edtechmagazine.com/higher/article/2012/07/how-save-money-time-and-sanity-mobile-device-management-software .

[27] Blustain, Harvey, Janice M. Abraham, Rebecca L. Adair, Elisabeth J. Carmichael, Glenn Klinsiek, and Jane W. Thompson, "Risk Management," in *College & University Business Administration* (Washington DC: National Association of College and University Business Officers).

[28] Schwartz, Karen D., "How to Save Money."

[29] Ahubia, Mor, "Two-Factor Authentication Gaining Traction in Higher Education," *SafeNet*, (March 6, 2014), http://data-protection.safenet-inc.com/2014/03/two-factor-authentication-gaining-traction-in-higher-education/#sthash.9bynOYyz.y6YBY6rx.dpbs.

[30] Burke, Steven and James McMahon, "Two-Factor Authentication," U.S. Department of Education (2015), http://ifap.ed.gov/presentations/attachments/56TwoFactorAuthenticationV1.pdf.

[31] Ibid.

[32] "Cyber Security," National Association of Insurance Commissioners and The Center for Insurance Policy and Research, (February 15, 2015), http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

[33] "A Buyer's Guide to Cyber Insurance," (October 2, 2013), http://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[34] Ibid.

[35] Ibid.