

Hacked!

BEST PRACTICES FOR PREVENTING AND RESPONDING TO DATA BREACHES AT YOUR SCHOOL

By William E. Hannum III and Arabela Thomas

If your school's Director of IT told you today that one of your school's talented, creative, and ambitious students hacked into your school's IT network and accessed the database holding student grades, tuition data, and donor information, including financial account numbers, what would you do?

As more and more independent schools move toward electronic storage of vital student, employee, and donor records, we continue to receive reports of data breaches similar to the one described above. Sometimes the hacker is not a student but a disgruntled

former employee or a stranger looking for financial account numbers. Other times, the data breach isn't intentional but results from an accidental loss of a laptop or a USB flash drive containing personal information.

Data breaches can have a significant impact on an independent school's relationships with its students, alums, and their families, as well as with faculty, staff, and other employees. Those affected may lose trust in the institution, given its apparent inability to safeguard sensitive, personal information. While the appropriate response to a data breach depends on the facts of the situation and applicable state and federal laws, below is a broad, step-by-step approach to help your school prepare for and respond to a data breach.

101101010101010111010110101101011
010111011101000111011101101010101
011010101010101010101010101110101
01010101011101010101010101010101
0111101011010011101011101011101
1100101011110111011101110111011
1011011101110111011101110111011
1011010101
0101110111010001110111011101110
0110101010101010101010101010101
0101010101110101010101010101010
0111101011010101010101010101010
1100101011110111010101110101011
1011**PASSWORD**0111010101110101011
1011010101010101010101010101010
0101110111010101010101010101010
0110101010101010101010101010101
0101010101110101010101010101010
0111101011010011101010101010101
1100101011110111011010111011101
10110111011010110110101111011011
10110101010101010111010110101101
0111101010101010101010101010101

1

PROMPTLY NOTIFY YOUR SCHOOL'S LEGAL COUNSEL.

Among other considerations, the school may be subject to data-breach notification requirements that call for prompt action. Your legal counsel should be able to help you and your school's crisis management team comply with any requirements and devise a comprehensive strategy for responding to the breach.

46 states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have enacted data-breach notification laws. In most cases they apply only when certain types of information are compromised. Massachusetts law, for example, imposes notification obligations when there is a

of notification methods that are acceptable. For example, while Missouri law allows "telephonic notice" of a breach to affected consumers (so long as the notice is provided directly to the consumer), telephonic notice is insufficient under the Massachusetts law.

Depending on the information compromised in a data breach, your school may also be required to comply with the data-breach laws of other states. If your school experiences a data breach involving names and social security numbers of Massachusetts residents, for example, it is obligated to comply with Massachusetts law even if the school is located outside of Massachusetts. Therefore, when assessing your school's notification obligations, it is important to consider (in consultation with your legal counsel) the resi-

dencies of all affected individuals and all of the various data-breach laws that may be applicable. Since many independent schools draw students from other states, these laws often require that notifications be sent around the country.

In addition to notification requirements under state laws, other data-breach notification requirements may also apply, depending on your school's operations and the types of information compromised. For example, if your school's health center experiences a data breach, and if it is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), then you may be required to provide notification in accordance with the federal Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). Additionally, your school may also be a party to contracts that require it to provide notification of breaches to the other contracting parties. For example, if your school's health center treats students from a neighboring school, the contract with that school may require you to notify it of a data breach affecting its students.



security breach or unauthorized acquisition or use of "personal information," which is defined as a state resident's "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password..." On the other hand, Missouri law defines "personal information" more broadly to include medical information or health insurance information combined with an "an individual's first name or first initial and last name."

State data-breach notification laws vary in a number of other ways, including who must be notified, the information that must be included in the notification, and the types

2

QUICKLY ASSESS THE NATURE AND SCOPE OF THE BREACH, INCLUDING INFORMATION COMPROMISED AND PARTIES AFFECTED.

Generally, this requires identifying and examining all of the affected data and devices as well as interviewing any individuals who may have information about the breach. During this fact-gathering process your school's legal counsel should provide you with guidance on preserving evidence relating to the breach and documenting the steps taken to contain and investigate it.

Legal counsel should also be involved in the fact-gathering to provide protection under the attorney-client privilege, to the greatest extent possible. The nature and scope of the available protection will vary under state law and with the circumstances; however, having an attorney involved will



Schools and Risk

Who do you look to for answers?

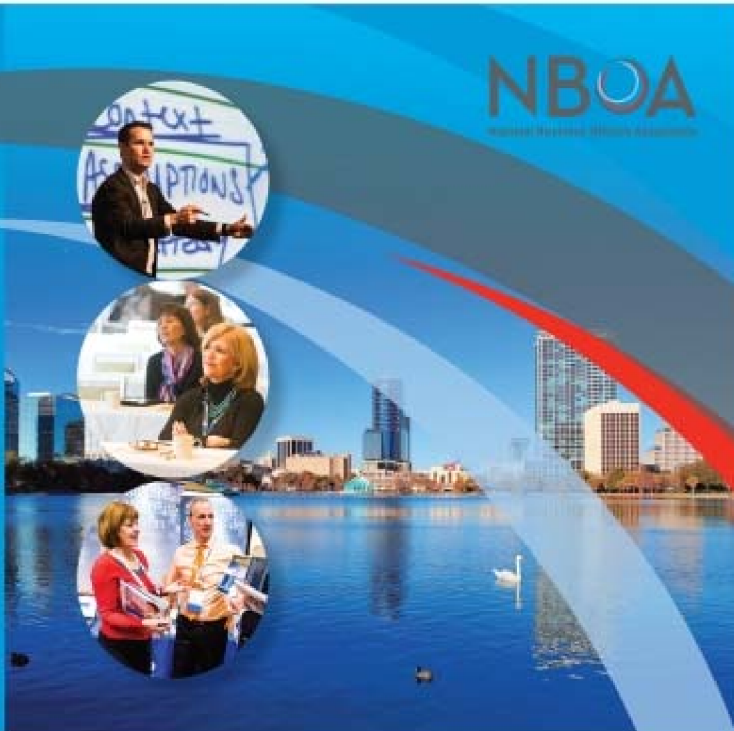
WRM AMERICA IS NOW **WRIGHT SPECIALTY INSURANCE**

The right partnership for you.[®] Wright Specialty Insurance is more than an insurance provider; we are a team of professionals—innovators devoted to finding solutions to the complex risks educational institutions face today. We provide loss reduction and cost containment strategies that deliver reduced premium rates and expanded coverage. Most importantly we are there with the expertise and claims excellence you need.

To find out more about how Wright Specialty can help you, visit our website:
www.wrightspecialty.com/policyholders.html

1.877.976.2111 | www.wrightspecialty.com

Wright Specialty Insurance is a member of The Wright Insurance Group. © Copyright 2012 The Wright Insurance Group. All rights reserved.


2014

NBOA Annual Meeting

March 2-5, 2014
 Orlando, FL
 Gaylord Palms

www.nboa.net

This year, the NBOA Annual Meeting will take place AFTER, not before, the NAIS Annual Conference. Registration opens October 1.

offer some protection, whereas there will be no such protection if an attorney is not involved.

If criminal activity is suspected (e.g., the data breach is apparently the result of a break-in or hacking), then it is often appropriate to notify law enforcement officials of the data breach so that they may guide or lead the investigation process and provide input regarding notification of affected parties. If a student hacks into the school's computer network, for example, law enforcement may be interested in speaking with the student and the student's parents before the school speaks to them or notifies them (and the rest of the school community) about the data breach. We generally recommend designating the school's legal counsel or a trusted member of the school's crisis management team as the primary contact for law enforcement and any relevant government agencies. The school should ensure that its designated contact has up-to-date information at all times concerning the school's investigation of and response to the data breach.

3 PROVIDE REQUIRED NOTIFICATIONS AND BE READY FOR QUESTIONS.

In addition to notifying affected individuals, many states' laws also require notification to designated government agencies and consumer reporting agencies. Under the North Carolina data-breach law, for example, an independent school that experiences a security breach must also notify the Consumer Protection Division of the North Carolina Attorney General's Office. Moreover, if pursuant to the North Carolina data-breach law the school provides notification to more than 1,000 people at one time, the school also must notify all consumer reporting agencies that compile and maintain files on

consumers on a nationwide basis (e.g., Equifax, Experian).

Whenever possible, the affected individuals should first learn of the data breach via the school—not via the media. As your school provides any legally required notifications, it is important to have a clear strategy for addressing questions that are likely to result from them. Although in most cases schools that experience a data breach are not required to provide free credit monitoring to the affected individuals, doing so may improve public relations and demonstrate your school's commitment to a just outcome.

4 USE THE DATA BREACH AS A LEARNING OPPORTUNITY.

Given the 20/20 vision of hindsight, it is helpful to analyze exactly what went wrong and how your school can improve its policies and procedures to prevent future data breaches. Does your school have a written policy regarding data security? Was the policy followed in this particular case? If not, why not? Should an employee who did not follow the school's policy be disciplined? Does the school have an acceptable use policy for its students? Was the policy violated? Should the student who violated it be disciplined? Asking these and other questions may help your school minimize the likelihood of another breach.

Earlier this year, a school experienced a data breach when a faculty member left in his car a USB flash drive containing students' names, Social Security numbers, and other sensitive information. The car was broken into and the USB flash drive was stolen. On examining school policies, administrators decided not to discipline the employee because the policies at the time of the breach did not prohibit employees from transporting unencrypted student information on portable devices.

As this example suggests, adopting a comprehensive data security policy can help your school not only to minimize the likelihood of a breach but also to respond appropriately if a breach occurs.

Your school's data-security policy should specify precautions employees must take when accessing, storing, and transporting personal information. The policy should also discuss the school's strategy for protecting personal information that is accessed or stored by the school's third-party service providers. For example, the school may contract with a third party to administer its employees' flexible spending accounts. If the school provides that third-party administrator with employees' personal information, the school may need to include a contract provision requiring the





administrator to protect such information in accordance with all applicable laws and to notify the school if the security of the information is breached.

In addition to adopting written policies pertaining to data security, it is also helpful for schools to provide employees with regular training about policies and procedures for protecting personal information and responding to data breaches. Employees should be informed of the potential consequences of their noncompliance with the school's data-security policies and procedures and the potential impact their noncompliance may have on the school's relationships with

the school community. Students should also be informed about the acceptable and unacceptable uses of technology and the consequences of violating the school's technology policies and procedures.

Preparation is key to preventing and responding effectively to data breaches. Updating data-security policies and procedures with the help of experienced counsel and IT professionals will give your school a fighting chance to minimize damage from a hack attack. ■



William E. Hannum III is the Managing Partner of Schwartz Hannum PC, which represents independent schools, colleges and universities in connection with education law and labor and employment matters.



Arabela Thomas is an attorney at Schwartz Hannum PC. Arabela is a magna cum laude graduate of Boston College Law School, where she was an editor for the Boston College Law Review.

Your Current Endowment Strategy May Not Add Up



Many investment experts agree that the coming years are going to be characterized by slow economic growth and below average returns from both stocks and bonds. This may leave independent schools struggling to find investment solutions that will protect their endowments' purchasing power, while generating the level of returns required to sustain long range spending goals. At ORION, we design forward-thinking investment strategies to prepare your endowment for the challenges ahead.

How do we do it?

- With independent, objective advice to help your school implement an investment plan designed to meet the highest fiduciary standards
- By giving you access to a broad universe of asset managers at significantly reduced minimums and fees
- By bringing to you the research and resources of Callan Associates, one of the world's largest investment consulting firms
- By providing your school with the timely and concise reports intended to ensure your funds are on target

An evolving world demands and evolving investment strategy. We can help.



2010 Corporate Ridge #560
McLean, VA 22102
(703) 720-5990
info@orionria.com

30 S. Wacker Drive #2200
Chicago, IL 60606
(312) 466-7592
www.orionria.com



All investment strategies have the potential for profit or loss.