FCSRMC

FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

Florida College System Roundtable Discussion

February 03, 2015

Cyber Overview

FCSRMC

FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

#1

CYBER RISK GENERAL OVERVIEW

What are the potential cyber risk exposures for your College?

Potential Risk

1. Breach of Personal Protected Information (PPI) / Hacker
2. Lost or Stolen Laptop/ Smartphone/ Tablets
3. Employee Negligence/ Human Error/ Rogue Employee
4. Thumb drives / Flash drives
5. Servers and Cloud Storage
6. Dropbox
7. Paper Files
8. Copy Machines

Potential Exposures

1. Student & Alumni Records
2. Enrollment Records
3. Social Security Numbers
4. Employee Records
5. Employee Benefit Records
6. Credit Card Numbers

FCSRMC
FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

#2

CYBER LIABILITY GENERAL OVERVIEW

What does cyber liability cover?

Breach Response Expenses
Covers crisis management, including notification cost, credit monitoring service, and public relations expenses incurred resulting from a security or privacy breach.

Data Restoration
Pays the costs for the restoration of any data stored.

Network Security Liability
Provides liability coverage for damages and claim expenses arising out of an actual or alleged act.

Privacy Liability
Provides liability coverage if an insured fails to protect personal protected information.

Privacy Regulatory Proceeding
Provides coverage for defense expenses from a regulatory proceeding resulting from a violation of a privacy law caused by a covered security breach.

Media Liability
Covers the insured for Intellectual Property and Personal Injury perils that result from an error or omission in content on their website.

Cyber Extortion
Provides coverage for expenses and/or losses incurred as the result of an extortion threat.

Business Interruption
Provides coverage for business interruption loss and/or business restoration expense as result of a security breach that caused system failure.

FCSRMC
FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

#3 BREACH RESPONSE PROCESS

How would my coverage respond in the event of a cyber liability claim?

Breach Response Timeline

1. Notify the Cyber Liability carrier once your organization is made aware of a possible breach.
2. The carrier will assign a Breach Coach to your organization who will help you select the proper breach counsel and forensic team.
3. The Breach Coach and your organization will select a notification service provider to notify the affected individuals ensuring all regulatory requirements are met.
4. Your organization will approve the notification letters to be mailed to the affected individuals.
5. The Breach Coach will contract a call center service provider to handle any questions on your organization's behalf.
6. Affected individuals receive their notification letters and may enroll in the credit monitoring service.
7. Your organization will receive reports on the progress of the notification letters and credit monitoring enrollment for continuous monitoring of the event.

FCSRMC
FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

What could a cyber breach cost you?

$188 - $194
Average cost per record (includes response costs, credit monitoring, forensics, and breach coach).

$5.4 Million
Average total cost per breach.

**2013Annual Study: U.S. Cost of Data Breach—by The Ponemon Institute, LLC; Sponsored by Symantec*

Your FCSRMC Team

Chauncey Fagler, ARM-P
Executive Director
Cfagler@FCSRMC.com
352-955-2190x101

Joshua Davis
Enterprise Risk Manager
Jdavis@FCSRMC.com
352-955-2190x114

Your Gallagher Brokerage Team

Peter Doyle
Area President
Peter_Doyle@ajg.com
678-393-5202

Michele Montgomery, CPCU
Area Vice President
Michele_Montgomery@ajg.com
407-563-3517

Johanne Daguillard
Client Service Manager
Johanne_Gaguillard@ajg.com
407-563-3535

Michael Gillon, ARM
Area President
Michael_Gillon@ajg.com
407-563-3550

Your Gallagher Cyber Team

Adam Cottini
Managing Director, Cyber Practice
Adam_Cottini@ajg.com
212-994-7048

Michael Guzman, ARM
Account Executive
Michael_Guzman@ajg.com
407-563-3555

Jennifer Boiling
Regional Director, Cyber Practice
Jennifer_Bolling@ajg.com
205-986-7711

FCSRMC
FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

College Data Breach Triples in Cost to Nearly $20 Million; Tuition Raised

Tagged: maricopa county community college

Thu Pham

Jun 2, 2014

What's a data breach cost these days? If you're Arizona-based Maricopa County Community College (MCCCD), it could cost you up to $19.7 million. In the wake of a data breach from early 2013, the college had initially anticipated spending up to $7 million total. A year later, that number has nearly tripled to take into account the countless fees that have added up to the gross amount of money spent mitigating the fallout.

FCSRMC

FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

Fitch Wire

View All Articles

share: email

07 Oct 2014 1:19 PM

Hacking Epidemic Puts US Colleges and Universities at Risk

Fitch Ratings-New York-07 October 2014: Cyber-attacks are becoming more prevalent at U.S. colleges and universities and media attention surrounding an attack poses reputational risk that could push down enrollment, according to Fitch Ratings.

Smaller private institutions with less resources and more operating challenges may have weaker security systems in place and a less prepared management team. Larger institutions with greater resources and strong management practices are likely better prepared to deal with or prevent them, due to the scale of their operations. Both large and small institutions could be more at risk if such an event were to occur given the sector's public profile and the negative publicity surrounding this type of event.

Institutions with insurance policies that specifically cover cyber-attacks in addition to traditional insurance may be better prepared to deal with an attack. However, preventative and post-event costs could include fraudulent charges not fully offset by insurance.

Colleges and universities are likely to remain attractive to hackers as enrollment and financial aid applications include students' and their parents' personal information, including their addresses, birth dates, social security numbers and proof of income. Further, online portals for tuition and other payments are sometimes linked to credit card and bank account information and passwords. We believe the security of systems and the investment in technology, in addition to the awareness of management, should be at the forefront of an institution's agenda.

The pace and size of breaches may also be rising. There have been approximately 29 data breaches at educational institutions since 2005. Before 2010, they were relatively small, with losses in the range of 100,000 records. But in 2013, Maricopa County Community College District lost 2.49 million records, and so far this year, data breaches have occurred at four colleges and universities.

SPECIALTY RISKS

January 18, 2015

SONY HACK SERVES AS WAKE-UP CALL, BOOSTS INTEREST IN CYBER SECURITY PROTOCOL

Issue NewsAsia-Pacific & AustralasiaRisk ManagementSpecialty RisksPolitical RiskTechnology

President Obama proposed cyber security legislation to Congress last week.

The cyber attack on Sony Corp. has been a wake-up call for many senior managers nationwide who were not already motivated by earlier hacking events.

They are reacting by making inquiries about their firm's cyber protection arrangements and seeking either to buy or increase insurance coverage, experts say. Meanwhile, insurers are expected to introduce stricter cyber underwriting standards before insuring a business.

President Barack Obama, who has blamed the Sony Pictures Entertainment Inc. hack on North Korea, introduced a cyber security legislative proposal to Congress last week that, among other provisions, calls for better cyber security information sharing between the private sector and government, as well as collaboration and information sharing within the private sector.

ebn

Obama cybersecurity plan could change healthcare processes

Proposed legislation the White House is sending to Congress to fight cyber attacks includes more protections for consumers than new requirements on companies to better protect the data that they hold. But one of the new requirements would appear to compel a major change in the HIPAA breach notification rule.

FCSRMC
FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

INSURANCE JOURNAL

View this article online:
http://www.insurancejournal.com/magazines/features/2014/09/22/340633.htm

The Ever-Evolving Nature of Cyber Coverage

To understand the current state of network security and privacy (cyber) coverage, it is helpful to have an understanding of the development and some of the major milestones which helped shape the coverage.

The first cyber policy was written in 1997 through AIG by Steve Haase, an agent who was recently awarded the "Advisen Cyber Legend Award." Though groundbreaking as the first to address cyber security, it was a third party liability policy only and was basically a "hacker policy."

Other very early entrants in writing cyber policies include Safeonline, CIGNA, Marsh and others. In the subsequent 17 years, internet use has grown from 1.7 percent of the global population in 1997 to an amazing 40 percent of the global population in 2014 resulting in dramatic changes since the first cyber insurance policy was written.

Currently, the total premium for cyber liability at year-end 2014 is projected to be nearly $2 billion. More than 60 carriers now offer stand-alone cyber policies and more are entering the market all the time. Many experts in this new field have appeared at the carrier, broker and wholesale levels. Experts are needed as each market/carrier has its own form with its own nuances and idiosyncrasies. Definitions for the same words differ on each policy form as do exclusions, terms and conditions.