


Cyber Liability Insight to Wisconsin Schools

Mark Meeks, CPCU, AIC

M3 Insurance

4/10/2014

Do You Recognize This Business?

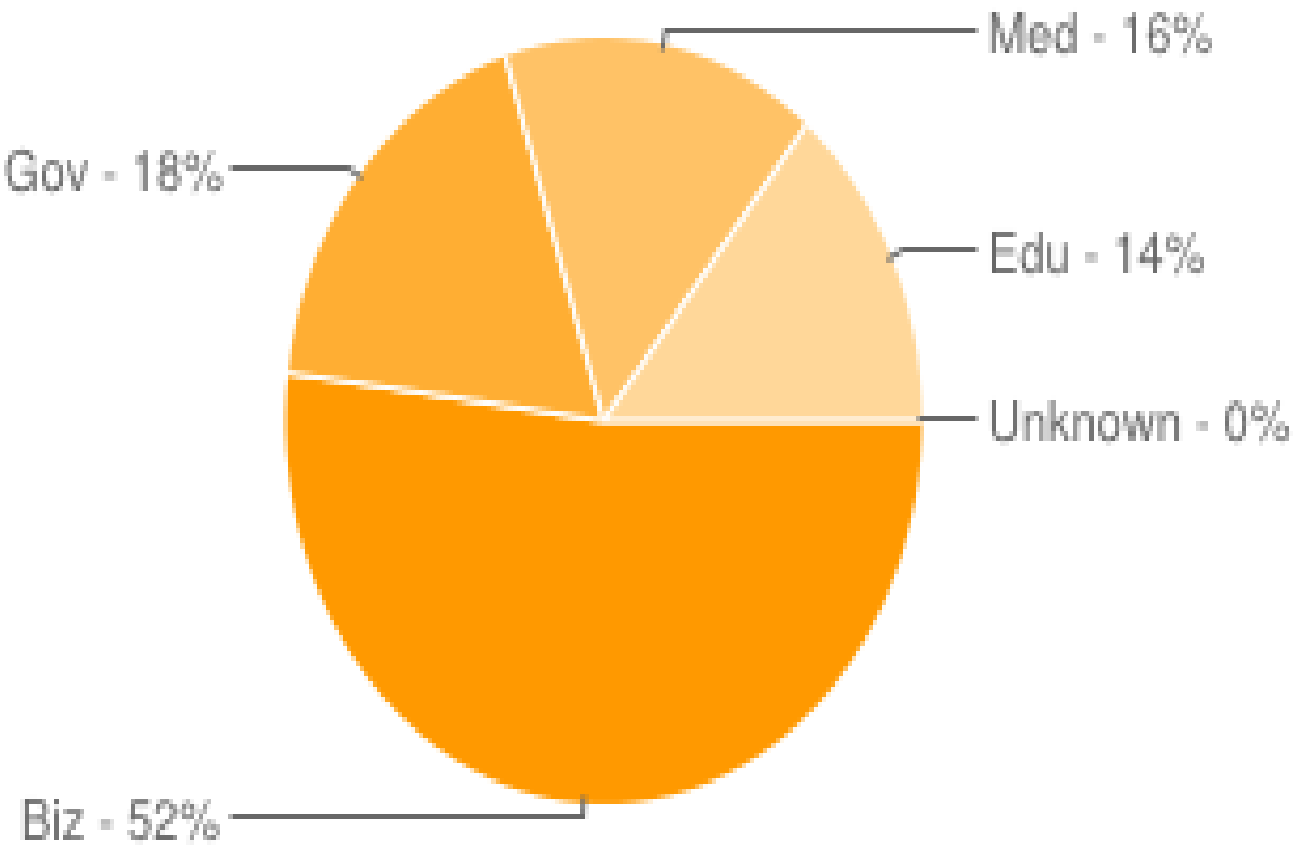
- Health Care Services
- Financial Services
- Computer Database Administration

This is Your District!

Kids will be Kids

- 2009 Survey by Panda Security
- 2010 Survey by Tuffin Technologies
- Orange County, California
- You Tube videos

Incidents by Business Type – All Time



Information obtained from dataloss db

Claims Involving School Districts

- 18,000 students' names, SS#, addresses, dates of birth, and parents' demographic information were available by searching Google. A private contractor unintentionally put student data on a computer Web server that was not secure.

- Identity thieves using the names and SS # of district employees made thousands of dollars in credit card purchases. At least 64 of the 3,400 teachers and other employees names were on an old benefits report that somehow ended up in the trash.

Claims Involving School Districts

- An instructor's grade book from 2001 to 2004 containing 303 students' SS#, among other personal information, was found to be compromised by a computer virus.

- School district accidentally sent out 5,000 postcards with students' SS# printed on the front. The district mailed 15,000 reminders asking parents to specify if they want to keep their children in magnet or traditional calendar schools. One third of the cards had the SS# printed alongside the child's name - a holdover from recent years when those nine-digit numbers were used to identify students.

District Regulatory Responsibilities

- Family Education Rights Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPPA)
- Fair Credit Reporting Act (FCRA)
- State and Federal Regulations Once a Breach Occurs – Wisconsin State Statute 134.98

Average Per Record Cost by Industry for Data Breach

Education	**$203**
Financial	$249
Healthcare	$294
Manufacturing	$136
Pharmacy	$310
Public sector	$90
Services	$256
Technology	$192
Transportation	$121

Source: Poneman Institute

Your Risks and Exposures

- First Party Risks
  - Cost to identify and fix the problem
  - Expenses to protect staff and families – including notification and credit monitoring costs
  - Public relations and legal expenses
  - Theft of data and intangible property
  - Cyber extortion

- Third Party Risks
  - Defense expenses
  - Damages resulting from lawsuits
  - Damages resulting from Regulatory fines or penalties

Risk Management

- Assess Your Risk
  - Prioritize, consider most critical data first.
- Implement Your Plan
  - Define your District's security risk appetite. What is your standard for security?
- Encrypt all important data such as financial information and employee social security numbers.
- Make sure all hardware is secure by physically locking down computers. If laptops are used, install tracking software.

Risk Management

- Adhere to PCI Security Standards

- Transfer potential risk by using the Cloud or third-party servers for data storage
  - Make sure the contract actually transfers risk

- Ensure WI-FI is securely locked with the latest encryption technology.

Risk Management

- Hackers used malware in half of all cyberattacks in 2010, install anti-malware and anti-virus software on all computers.
- Educate employees on your internet policy as well as the signs of a cyberattack.
- Review your current data compromise or cyber liability policy, understand what it covers and just as importantly, what it does not.

QUESTIONS?