

# CYBER LIABILITY WEBINAR

## May 12, 2010



**PRESENTED BY:**  
BLAIS EXCESS & SURPLUS  
AGENCY OF TEXAS, LTD.  
[WWW.BLAISEXCESS.COM](http://WWW.BLAISEXCESS.COM)



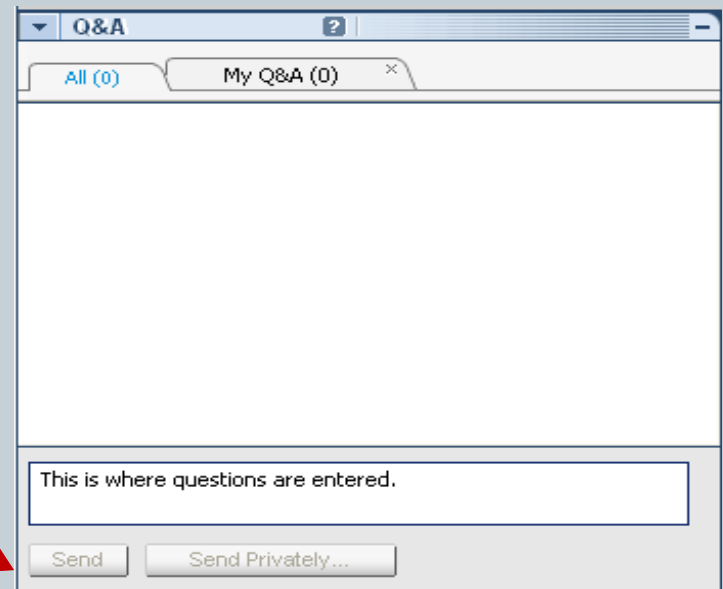
# Cyber Webinar Details



**Our webinar is being offered through an audio broadcast mode. Audio broadcast automatically starts when an attendee joins the event. Attendees can play, pause or stop the broadcast. Remember to take our mute button off your speakers if you cannot hear the presenter! Please adjust the volume on your speakers**

**The Q&A Panel can be used throughout the presentation.**

**Enter your question and then hit send.**

A screenshot of a web browser window titled "Q&A". The window has two tabs: "All (0)" and "My Q&A (0)". The main content area is empty. At the bottom, there is a text input field with the placeholder text "This is where questions are entered." Below the input field are two buttons: "Send" and "Send Privately...". A red arrow points to the "Send" button.

Q&A

All (0) My Q&A (0)

This is where questions are entered.

Send Send Privately...

# Cyber Webinar Panelists



**Vikki Robinson**

**Blais Excess & Surplus – Houston**

[vikki@blaisexcess.com](mailto:vikki@blaisexcess.com)

**Scott Stortzum**

**Blais Excess & Surplus – Houston**

[scott@blaisexcess.com](mailto:scott@blaisexcess.com)

# What is Cyber Liability?



- **Technology Errors & Omissions**  
(software programmers, technology consultants, ISPs, etc....)
- **Privacy & Security Coverage** (data breaches, loss of customer / patient information, etc...)

# Privacy Issues Can Produce a Cascade of Losses



## First Party

### Loss of Private Data

- Notification Costs
- Cost to Change Account Numbers
- Publicity Costs

### Cyber Extortion

- Ransom Payment
- Other Expenses

## Third Party

### Customer Suits

- Suits from Customers alleging invasion of privacy and other causes of action

### Other Suits

- Regulatory actions from Governmental Agencies

# Third Party Coverage



Policy responds to claims brought by third parties for a variety of actions:

- Information Security/Privacy Liability – theft, loss or unauthorized disclosure of non-public information in care/custody/control of NI
- Computer security issues – ie failure to prevent the transmission of malicious code from insured's computers to customer's computers
- Failure to timely disclose loss of non-public information
- Failure to comply with internal privacy policy issues
- Failure to administer identity theft prevention program required by statute or regulation

# First Party Coverage



Policy will pay/reimburse the named insured for costs incurred:

- **Privacy Notification Costs – incurred after a breach is discovered:**
  - hiring of security expert to determine existence/cause of breach
  - notification costs to individuals with compromised information
  - credit monitoring services to those with compromised information
  - costs for public relations consultants
- **Extortion Demands – ransom payments, reward monies, other expenses**

# A Sample Data Breach...



The Privacy Rights Clearinghouse is a non-profit organization that was created to (1) raise consumer's awareness about how technology affects privacy and (2) provide practical tips on privacy protection. They can be found at [www.privacyrights.org](http://www.privacyrights.org).

<b>Date Made Public</b>	<b>Name (Location)</b>	<b>Type of Breach</b>	<b>Number of Records</b>
12/30/2006	KeyCorp (Cleveland, OH)	A laptop computer stolen from KeyCorp vendor contains personally identifiable information, including SSNs, of 9,300 customers in six states	9,300

# Data Breaches – Growing in Number!



- Between January, 2005 and May 4, 2010

**353,812,819**

records containing “sensitive personal information”  
have been involved in security breaches!

*Source: Privacy Rights Clearinghouse A Chronology  
of Data Breaches.– updated April 26, 2010*

# Sources of Data Breaches...

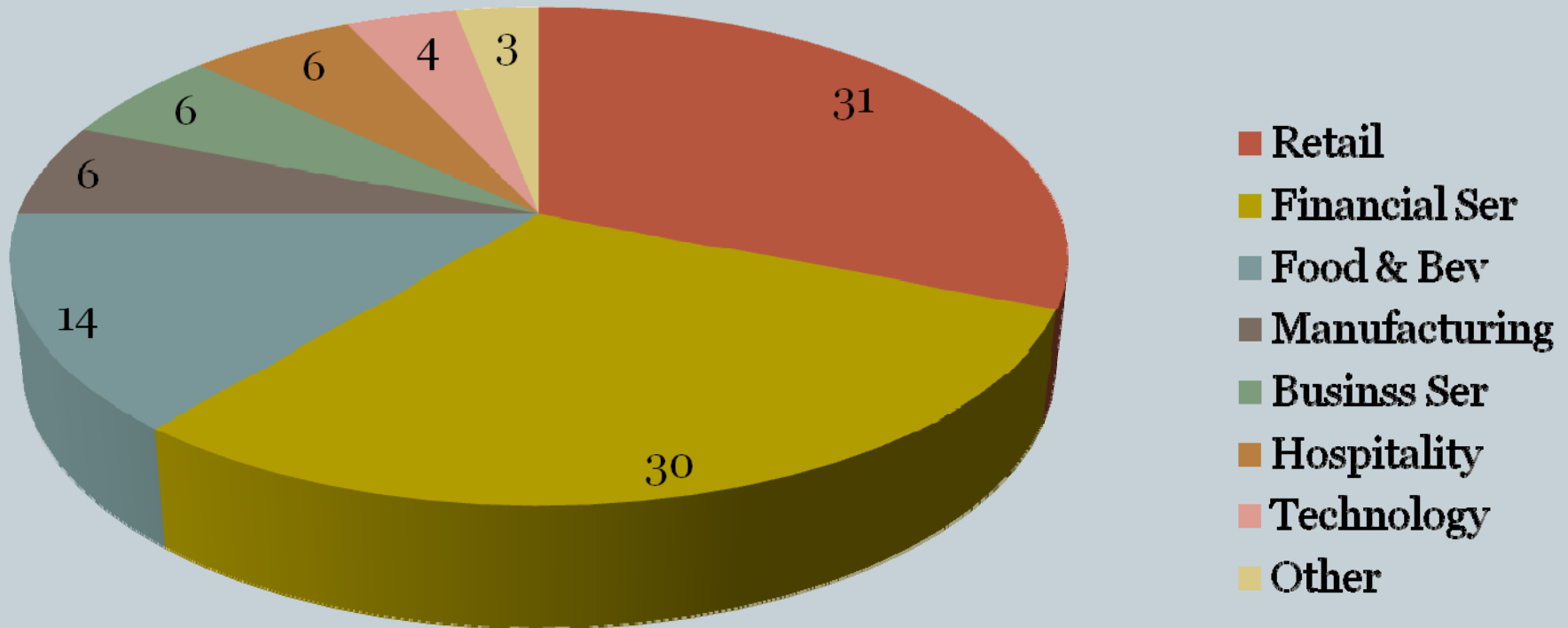


- Laptop Theft or other device – 33%
- Negligent Employee – 22%
- External Hackers – 15%
- System Failure – 10%
- 3<sup>rd</sup> Parties – Partner, Outsourcer – 10%
- Lost Media Backup – 5%
- Social Engineering – 5%

# Industries Most Affected



## % of Breaches in 2008



Financial Services breaches accounted for 93% of all records compromised in 2008

# What's the Cost?



- Notification Expenses average \$13 per lost record.
- Free or Discounted Services average \$24 per record.
- Other Expenses average \$16 per lost record
- ***Total for these Direct Expenses: \$53 per record!***

*Source: Ponemon Institute, LLC – “2008 Annual Study: Cost of a Data Breach”*

# Federal Regulations



- HIPAA
- Gramm Leach Bliley
- Federal Trade Commission Act

# State Notification Statutes



- California first state to enact “security breach notification” legislation – July 1, 2003 [SB 1386].
- As of January 2010, only 5 states do not have notification provisions (Alabama, Kentucky, Mississippi, New Mexico, South Dakota)
- Most states define a breach as unauthorized access to unencrypted, computerized personal information which is generally first name, or first initial and last name, plus (1) SSN# or (2) Driver’s License or (3) Financial account, credit or debit card number along with required access code or password

# Laptop Theft



***April 5, 2010***

- John Muir Physician Network  
(Walnut Creek, CA)
- Two laptop computers at the John Muir Physician Network Perinatal office in Walnut Creek were stolen. The laptops were password protected and contained data in a format that would not be readily accessible. External vendors and internal experts discovered that the missing laptops contained personal and health information going back more than three years.
- The network began notifying 5,450 patients by mail of the breach

# Possible Employee Dishonesty



***April 28, 2010***

- The Medical Center (Bowling Green, KY)
- The Medical Center at Bowling Green is notifying 5,418 patients whose medical information may have been breached when a computer hard drive was stolen. The computer hard drive was taken from the hospital's mammography suite and contained information from patients who underwent bone density testing between 1997 and 2009.

# Employee Negligence



***October 21, 2009***

- Bullitt County Public Schools (Shepherdsville, KY)
- A Bullitt County Public Schools employee accidentally sent an e-mail message to about 1,800 school district workers that included the names and Social Security numbers of 676 district employees. The employees were identified as not having completed the district's 2010 open-enrollment process for insurance, and the e-mail was intended as a reminder to complete the process.

# Stolen Computer Server



***June 14, 2006***

- American Insurance Group (AIG), Indiana Office of Medical Excess, LLC (New York, NY)
- The computer server was stolen on March 31 containing personal information including names, SSNs, birth dates and some medical/disability information.
- 930,000 records affected

# Security Breaches – Cyber Attacks



***May 28, 2008***

- University of California, San Francisco (San Francisco, CA)
- During routine monitoring of a campus computer network, UCSF discovered unusual data traffic on one of its computers. During the investigation, UCSF determined that an unauthorized movie-sharing program had been installed on one computer by an unknown individual. Installation of this program required high-level system access. The computer contained files with lists of patients from the UCSF pathology department's database. The data included information such as patient names, dates of pathology service, health information and, in some cases, Social Security numbers.
- 3,569 records affected

# Security Breaches – Hackers



***June 12, 2006***

- U.S. Department of Energy (Washington, D.C.)
- Names, Social Security numbers, security clearance levels and place of employment for mostly contract employees who worked for National Nuclear Security Administration may have been compromised when a hacker gained entry to a computer system at a service center in Albuquerque, N.M. eight months ago.
- 1,502 records affected

# Security Breaches – Hackers



***April 9, 2010***

- Charles Schwab (Albany, NY)
- A Russian national was sentenced to 37 months in prison for hacking into victims' brokerage accounts at Charles Schwab, laundering more than \$246,000 and sending a portion back to co-conspirators in Russia. The man also sold approximately 180 stolen credit card numbers to a cooperating witness and directed that they be fabricated into credit cards. According to the indictment, from approximately September 2006 through December 2007, two men participated in a scheme to steal funds from bank and brokerage accounts by hacking into those accounts through the Internet, using personal financial information obtained through a Trojan computer virus and then laundering the stolen proceeds.
- The total number of records affected at this time is unknown.

# Security Breaches – Theft



***May 23, 2008***

- R.E. Moulton (Irving, TX)
- Thieves broke into the Irving, Texas regional office and stole a laptop computer containing personally information of numerous individuals, including names and Social Security numbers.
- 19,000 records affected

# The Daily Headlines...



- **TIME WARNER:** Lost unencrypted computer backup tapes containing sensitive information from as far back as 1986 about 600,000 people, including Social Security numbers.
- **OHIO UNIVERSITY:** Faces a class-action lawsuit filed by two alumni whose personal data were among those accessed when hackers broke into OU's computer system.
- **DSW SHOE WAREHOUSE:** Announced that thieves had accessed 1.4 million credit card numbers, checking account numbers, and driver's license information of about 96,000 customers.
- **CHOICEPOINT, INC:** Announced that a fraud ring had gained access to approximately 145,000 records containing personal and financial information about consumers from the company's database. Subsequent reports indicated this was not the first such security breach at Choicepoint, an information broker.

# The Daily Headlines...



- **LIFETIME FITNESS:** Faces suit from the Texas Attorney General for failing to safeguard its customers personal data. During a 3 month period, more than 100 business records containing sensitive customer information were found in trash bins adjacent to various locations. The lawsuit seeks civil penalties of up to \$500 for each business record not properly disposed, of, up to \$50,000 for each violation of the Identity Theft Enforcement and Protection Act, up to \$20,000 for each violation of the Deceptive Trade Practices Act, and other penalties.
- **MONSTER.COM:** Recently acknowledged that intruders swiped sensitive data for at least 1.3 million job seekers. The Company faced expenditures to shut down servers and could face suit from users.
- ***Crimes like these happen almost every week...***

# Blais Excess & Surplus Agency of Texas Ltd.



*Note: This is designed to be a general overview of the coverage outlined above, and is not intended nor should it be construed as a complete explanation of the coverage that may be available. Different and/or additional terms and conditions may apply with respect to the coverage sought. Please read all policies carefully and contact your agent or broker with any questions.*

## **Houston Office**

820 Gessner  
Suite 1750  
Houston, TX 77024  
(713) 780-7787 *Phone*  
(713) 780-3533 *Fax*

## **Dallas Office**

14643 Dallas Parkway  
Suite 700  
Dallas, TX 75254  
(972) 818-4090 *Phone*  
(972) 818-4088 *Fax*

## **Austin Office**

P.O. Box 92824  
Austin, TX 78709  
(512) 894-3460 *Phone*  
(512) 858-1266 *Fax*

Website Address: [www.blaisexcess.com](http://www.blaisexcess.com)

# Copyright Notice



Copyright © 2010  
Blais E&S - Blais Aviation - RDAUS  
All Rights Reserved

The views expressed in this document are exclusively those of the author. All of the content in this document has been created solely in the author's individual capacity. This document may not be quoted unless the author has given his/her written consent in advance. This document does not intend to provide legal advice.



[www.blaisexcess.com](http://www.blaisexcess.com)