Nominee Showcase Presentation

ISE NORTH AMERICA LEADERSHIP SUMMIT

Nominee Showcase Presentation

November 17, 2011

Company Name:	University of California
Project Name:	"Reverse Underwriting" for Cyber Risk
Presenter:	Grace M. Crickette
Presenter Title:	Chief Risk Officer

T.E.N.
TECH EXEC NETWORKS

Nominee Showcase Presentation

Company Overview

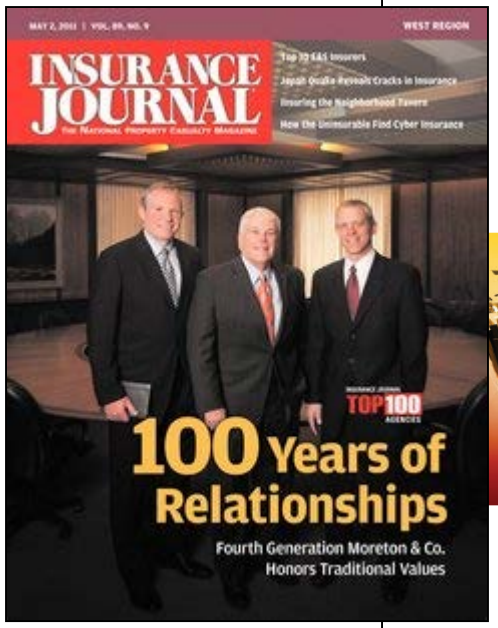
- The University of California's fundamental missions are teaching, research and public service
- 10 campuses, 5 medical centers, 3 national laboratories, 56 Agriculture & Natural Resource stations
- More than 220,000 students
- More than 170,000 faculty and staff
- Operating budget $22 Billion

Nominee Showcase Presentation

Presentation/Project Overview

- UC uninsurable
- Reverse underwriting
- Lessons learned & best practices

Nominee Showcase Presentation



WEST COVERAGE

News&Markets

How to Find Cyber Insurance for the Uninsurable

By Patricia-Anne Tom

The University of California (UC) has redefined the rules of cyber liability insurance, using an approach that the university's Chief Risk Officer Grace Crickette calls "reverse underwriting." Collaborating with the university's chief information officers, insurance brokers Price Forbes & Alliant, and a London underwriter, UC developed a cyber liability insurance program that reduces risk and drives risk management best practices, Crickette said.

Several years ago, the University of California Office of Risk Services was increasingly becoming aware of cyber risks, encompassing the exposures presented by network security, privacy and social networking. While the UC as well as cyber breach incidents.

"Due to the nature and complexity of operations and the academic culture of open access, educational institutions, and in particular, large research-oriented universities, face unique exposures related to the Internet and information security and privacy," according to a 2008 white paper on "Cyber Liability and Higher Education" by Aon Corp.

In 2008, educational institutions accounted for 33 percent of all reported data breaches. From Jan. 1, 2007 until Nov. 19, 2008, approximately 158 such institutions experienced data breaches involving 3.7 million records. The Ponemon Institute found the average cost of a data breach was $197 per record.

Such statistics put reducing cyber risks on UC Regents' radar, Crickette said. The problem she found, however, was that no insurer wanted to write UC's cyber liability coverage because she couldn't complete the insurance applications — or the answers made the university seem like a high risk.

For instance, some asked:

- Within the past three years, have you had a failure or breach of computer security systems that caused a loss in excess of $25,000?
- Have you had any losses due to

and 250,000 students. The university is heavily involved with research, and manages patient care and public services, such as operating 56 Agriculture and Natural Resource stations for the state of California.

"While core systems like payroll and accounting systems are centralized, not all IT systems are," Crickette said, "because of how funding comes to a university."

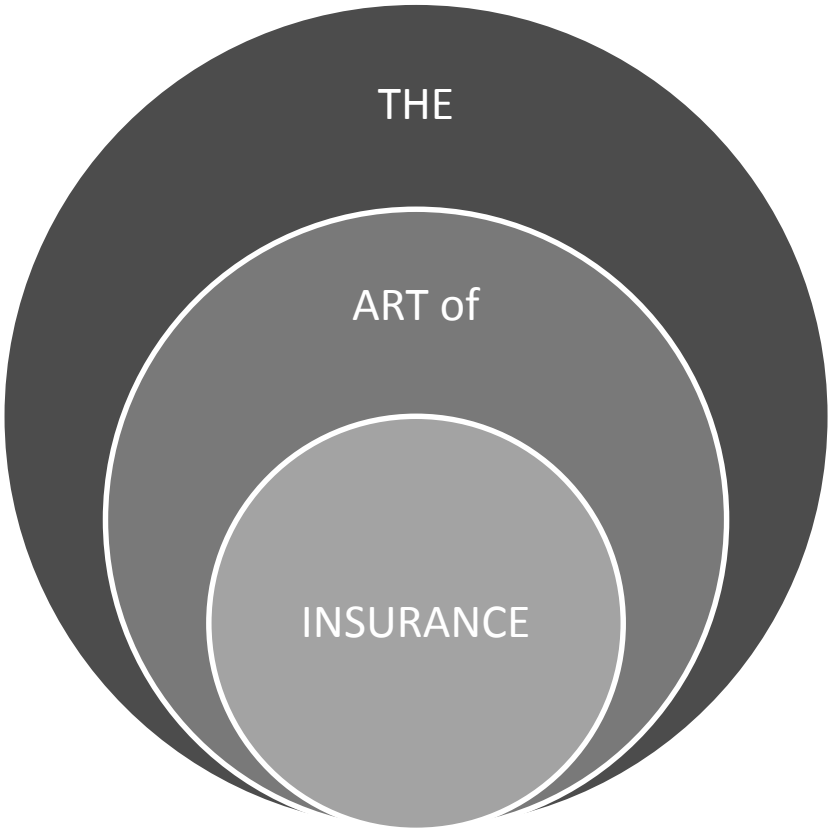
Often, a university receives much of its funding through research grants, from governmental agencies or private industry, she explained. Typically that money goes to a specific professor, also known as the "primary investigator" (PI), and monies do not go to the university's general fund.

"When a corporation has revenue that comes in, it goes into a general accounting fund, and senior leadership along with the board will make strategic decisions about how that money will be allocated. We don't have that luxury at the university," Crickette said. Instead, a significant amount of funding is "tagged" for a special purpose.

To complete and support the research, a PI may need a particular computer system or standalone server. The tendency is for each PI to have

Nominee Showcase Presentation

IT Meets Insurance



Nominee Showcase Presentation

The Threat

The Pentagon's second-in-command, Deputy Secretary William J. Lynn III, asserted that the threat to intellectual property of businesses, **universities** and the government may be “the most significant cyberthreat” facing the country. (*Washington Post,* Thursday, September 16, 2010)

Nominee Showcase Presentation

Go Gauchos!

- **UCSB Team Wins 2005 DEFCON Hacking Contest**
- UCSB team “Shellphish”, led by Professor Giovanni Vigna from the Department of Computer Science and composed of Computer Science graduate students, won the "Capture The Flag" competition at DEFCON
- DEFCON (http://www.defcon.org) is the largest underground hacker convention in the world
- The "Capture The Flag" competition is held every year as part of the convention and regarded as the “world championship of hacking”

Impact of Data Breach

- Direct Costs
- Discovery / Data Forensics
- Notification costs
- Identity monitoring costs
- Real-time crisis management costs
- Additional security measures, remediation
- Defense Costs/Settlements
- Regulatory fines
- Call Center Management
- Civil Suits

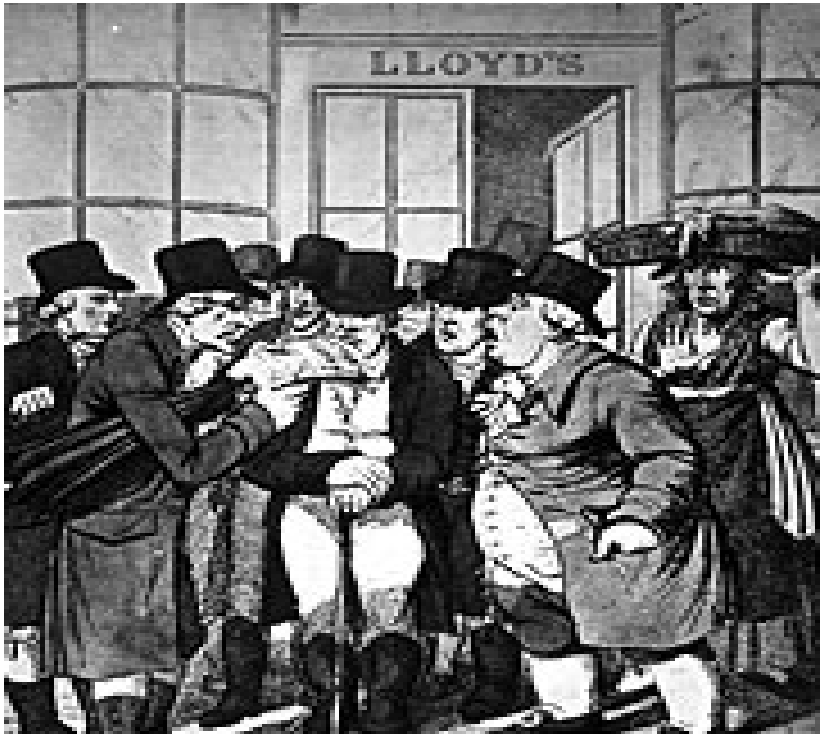
- Indirect Costs
- Loss of student/faculty confidence
- Executive management distraction from core objectives
- Loss of employee productivity
- Alumni impact, giving etc.
- Impact on enrollment
- Loss of management credibility

Nominee Showcase Presentation

Project/Program Scope/Goals

- Protecting against Cyber Risks should be an organizational commitment – ERM
- Insurance is becoming more available, but should be the last line of defense
- Traditional underwriting was not an option for UC
- CRO/Broker approached insurance markets regarding a new solution - reverse underwriting concept.

Nominee Showcase Presentation



Lloyd's coffee house became recognized as the place for obtaining marine insurance.

A Day at the Races

Nominee Showcase Presentation

How Premiums are Calculated

Exposures

How many?

What type?

Experience

Frequency

Severity

Time

How Premiums are Calculated

Loss Development Factors

External

Internal

Project/Program Results

"Reverse Underwriting":

- Underwrite to standards rather than to existing conditions
- Provide CIOs with a tool to drive improved behavior around cyber risk
- Provides first dollar insurance coverage for those that meet UC's policies – rewarding best practices
- Provides a secondary savings through consolidation of systems (utility cost, space, maintenance, IT redundancy)
- Supports improved post-loss Risk Response
- Supports proactive risk management tools and techniques

Nominee Showcase Presentation

Security & Privacy Insurance Policy Coverage Overview

Risks	Coverage	Existing Insurance Policies	Improved Insurance Policies
Legal liability to others for privacy breaches	Privacy Liability: Harm suffered by others due to the disclosure of confidential information		
Legal liability to others for computer security breaches	Network Security Liability: Harm suffered by others from a failure of your network security		
Loss or damage to data/ information	Property Loss: The value of data stolen, destroyed, or corrupted by a computer attack		
Loss of revenue due to a computer attack	Loss of Revenue: Business income that is interrupted by a computer attack		
Extra expense to recover/ respond to a computer attack	Cyber Extortion: The cost of investigation and the extortion demand		
Loss or damage to reputation			
Identity Theft	Expenses resulting from identity theft		
Privacy Notification Requirements	Cost to comply with privacy breach notification statues		
Regulatory Actions	Legal defense for regulatory actions		

Legend: No coverage | Limited coverage | Full coverage

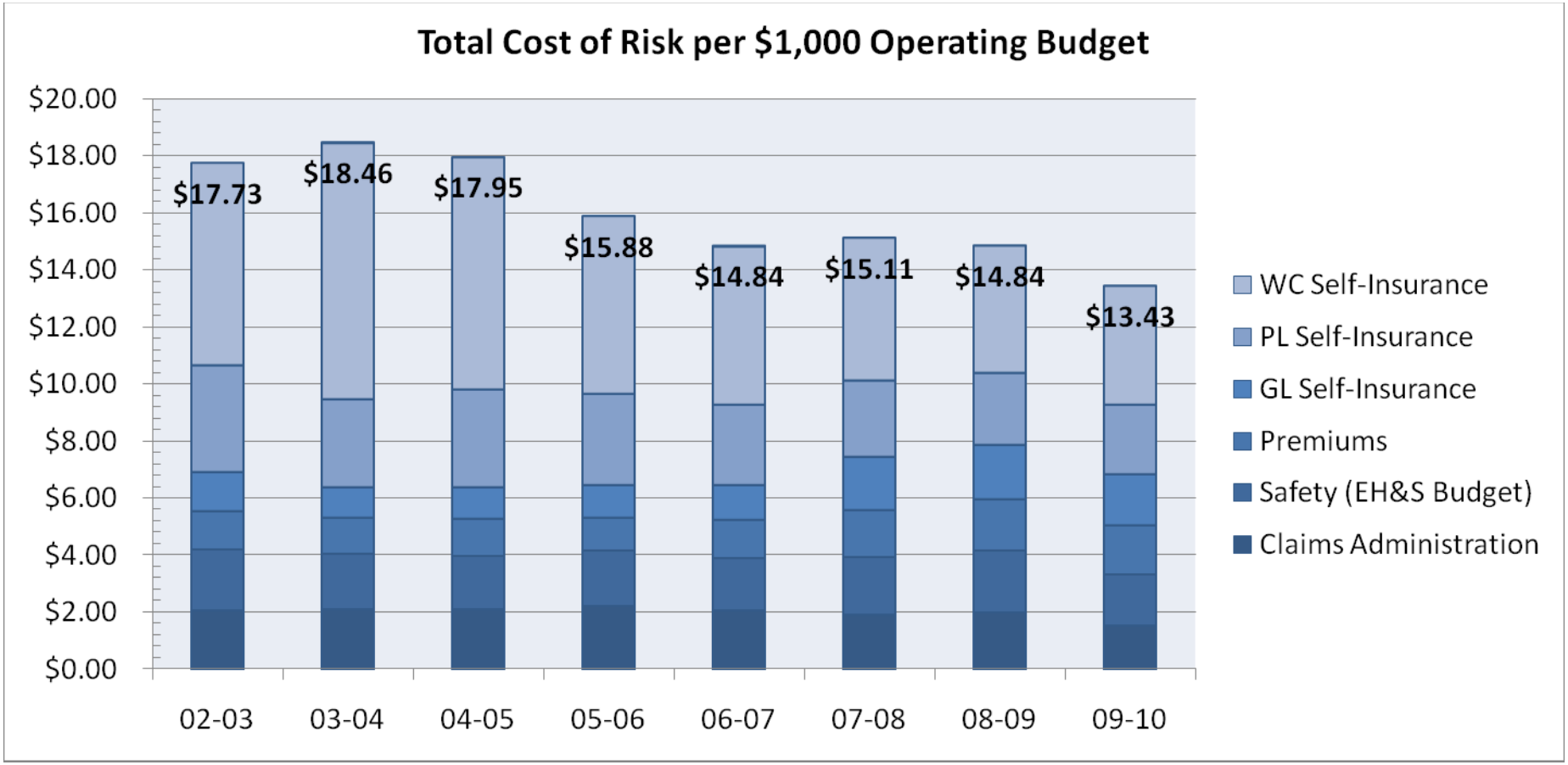
Nominee Showcase Presentation

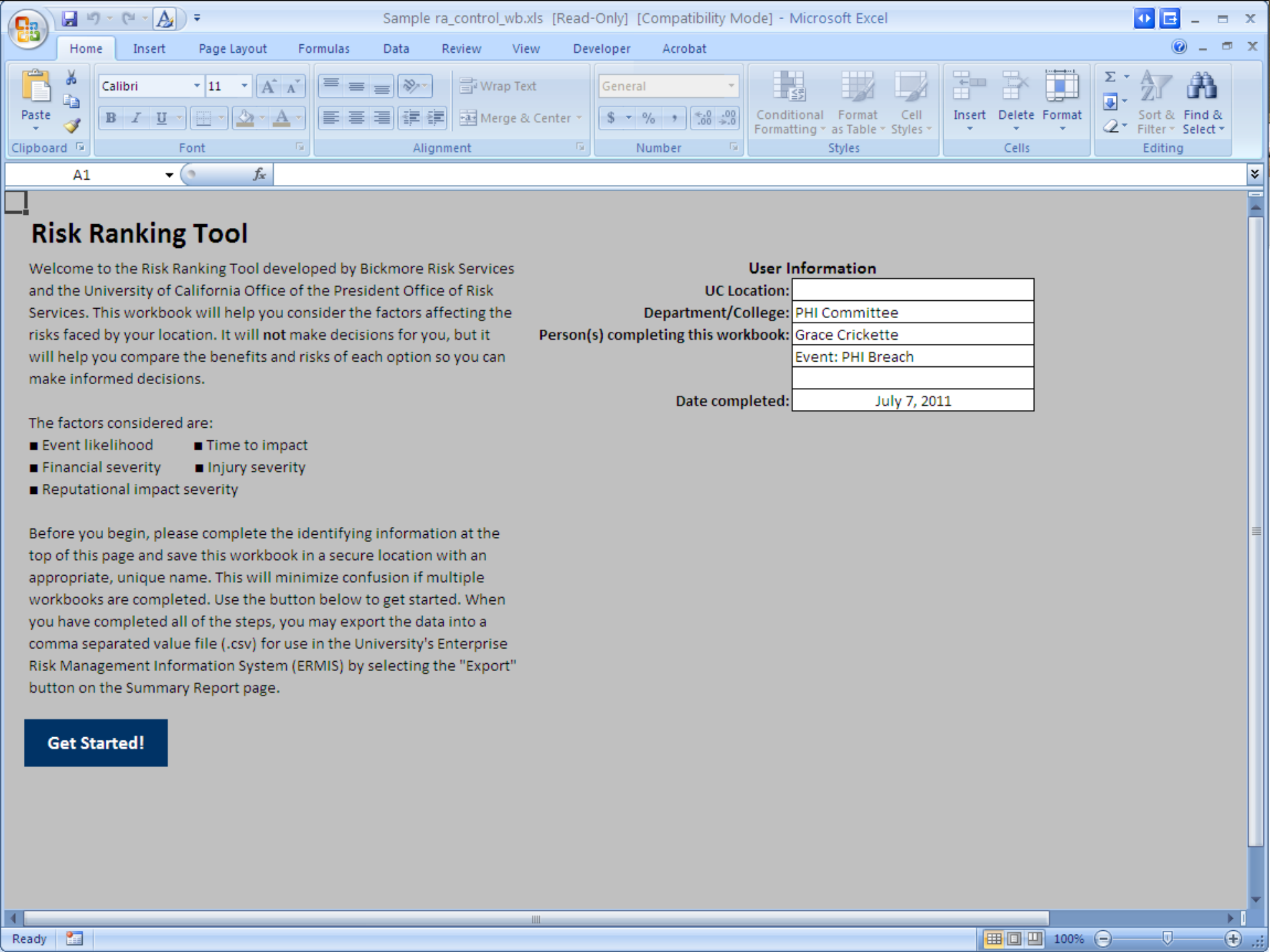
Cyber Insurance Coverage Limits

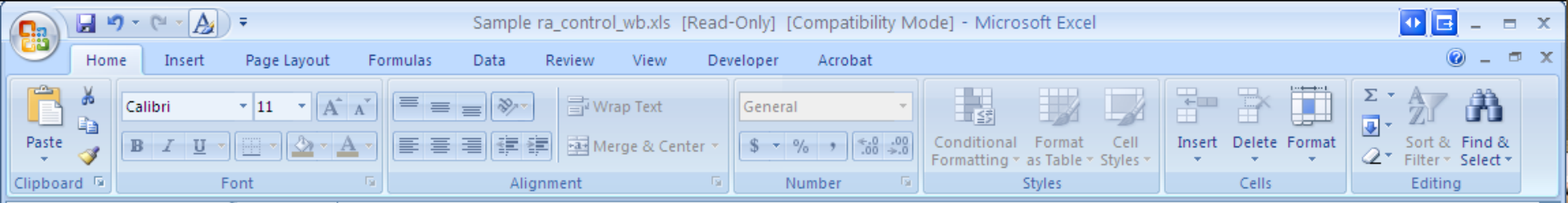
Property- **$5 Billion Limits** **$7.5 Million deductible** Covers physical loss or damage to hardware and software.	**Liability-** **$275 Million Limits** **$2.5 Million deductil** Covers negligent acts or omissions.	**Cyber/Privacy Breach-** **2011 - $10 Million Aggregate for same premium** Covers damages and expenses caused by a privacy, confidentiality or security breach.

First dollar coverage for campuses within self-insurance program

Nominee Showcase Presentation




Sample ra_control_wb.xls [Read-Only] [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Developer
Acrobat
Paste
Calibri
11
Wrap Text
General
Merge & Center
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipboard
Font
Alignment
Number
Styles
Cells
Editing
A1
Risk Ranking Tool
Welcome to the Risk Ranking Tool developed by Bickmore Risk Services and the University of California Office of the President Office of Risk Services. This workbook will help you consider the factors affecting the risks faced by your location. It will not make decisions for you, but it will help you compare the benefits and risks of each option so you can make informed decisions.
The factors considered are:
■ Event likelihood
■ Time to impact
■ Financial severity
■ Injury severity
■ Reputational impact severity
Before you begin, please complete the identifying information at the top of this page and save this workbook in a secure location with an appropriate, unique name. This will minimize confusion if multiple workbooks are completed. Use the button below to get started. When you have completed all of the steps, you may export the data into a comma separated value file (.csv) for use in the University's Enterprise Risk Management Information System (ERMIS) by selecting the "Export" button on the Summary Report page.
Get Started!
User Information
UC Location:
Department/College: PHI Committee
Person(s) completing this workbook: Grace Crickette
Event: PHI Breach
Date completed: July 7, 2011
Ready
100%



Return to Introduction
Evaluating Risks
Step 1: Identify Potential Risk Events
Step 2: Estimate Event Likelihood
Step 3: Estimate Time to Impact
Step 4: Estimate Financial Severity
Step 5: Estimate Injury Severity
Step 6: Estimate Reputational Severity
Reports
Summary
Chart of Events

Potential Risk Events	Likelihood Factor	Impact of Controls
Patient Self-Censoring of Information	Occurs periodically	Minor
Employee Theft or Misuse of PHI	Extremely rare	Minor
Publication of Facts re Breach	Very common	Moderate
Employee Termination	Very common	Substantial
Decrease in referrals	Occurs periodically	Moderate
Increased audits	Very common	Minor

Step 2: Estimate Event Likelihood

Estimate the likelihood of each event occurring using the scale below:

Extremely rare
Once every 25 years or more

Occurs rarely
Once every 6-25 years

Occurs periodically
Once every 2-5 years

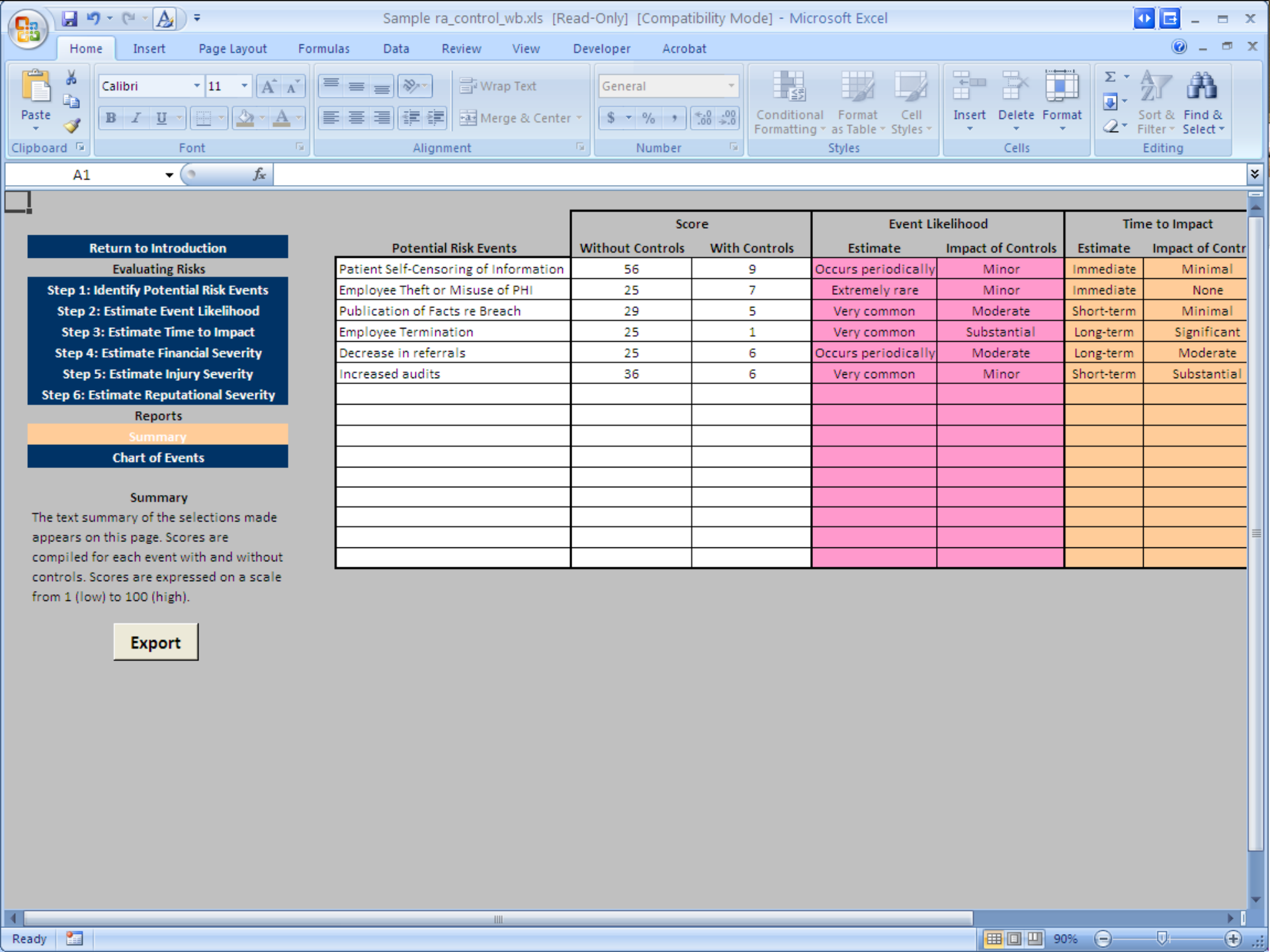
Occurs regularly
Every year

Very common
Multiple times each year

Next, estimate how proposed controls impact how likely the event is to occur.

Nearly complete - Reduced by 99%
Significant - Reduced by 90%
Substantial - Reduced by 70%
Moderate - Reduced by 50%
Minor - Reduced by 30%
Minimal - Reduced by 10%
None - Not reduced at all
Unsure/Don't know

Customize Scales


Sample ra_control_wb.xls [Read-Only] [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Developer
Acrobat
Paste
Calibri
11
Wrap Text
General
Merge & Center
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Sort & Filter
Find & Select
Clipboard
Font
Alignment
Number
Styles
Cells
Editing
A1
Return to Introduction
Evaluating Risks
Step 1: Identify Potential Risk Events
Step 2: Estimate Event Likelihood
Step 3: Estimate Time to Impact
Step 4: Estimate Financial Severity
Step 5: Estimate Injury Severity
Step 6: Estimate Reputational Severity
Reports
Summary
Chart of Events
Summary
The text summary of the selections made appears on this page. Scores are compiled for each event with and without controls. Scores are expressed on a scale from 1 (low) to 100 (high).
Export
Potential Risk Events
Score
Without Controls
With Controls
Event Likelihood
Estimate
Impact of Controls
Time to Impact
Estimate
Impact of Contr
Patient Self-Censoring of Information 56 9 Occurs periodically Minor Immediate Minimal
Employee Theft or Misuse of PHI 25 7 Extremely rare Minor Immediate None
Publication of Facts re Breach 29 5 Very common Moderate Short-term Minimal
Employee Termination 25 1 Very common Substantial Long-term Significant
Decrease in referrals 25 6 Occurs periodically Moderate Long-term Moderate
Increased audits 36 6 Very common Minor Short-term Substantial
Ready
90%

Return to Introduction

Evaluating Risks

Step 1: Identify Potential Risk Events

Step 2: Estimate Event Likelihood

Step 3: Estimate Time to Impact

Step 4: Estimate Financial Severity

Step 5: Estimate Injury Severity

Step 6: Estimate Reputational Severity

Reports

Summary

Chart of Events

Chart of Events with Controls

The chart here shows the risk events arrayed based upon the selections made below. *Selections in parentheses () use figures calculated without controls.*

Vertical Axis:

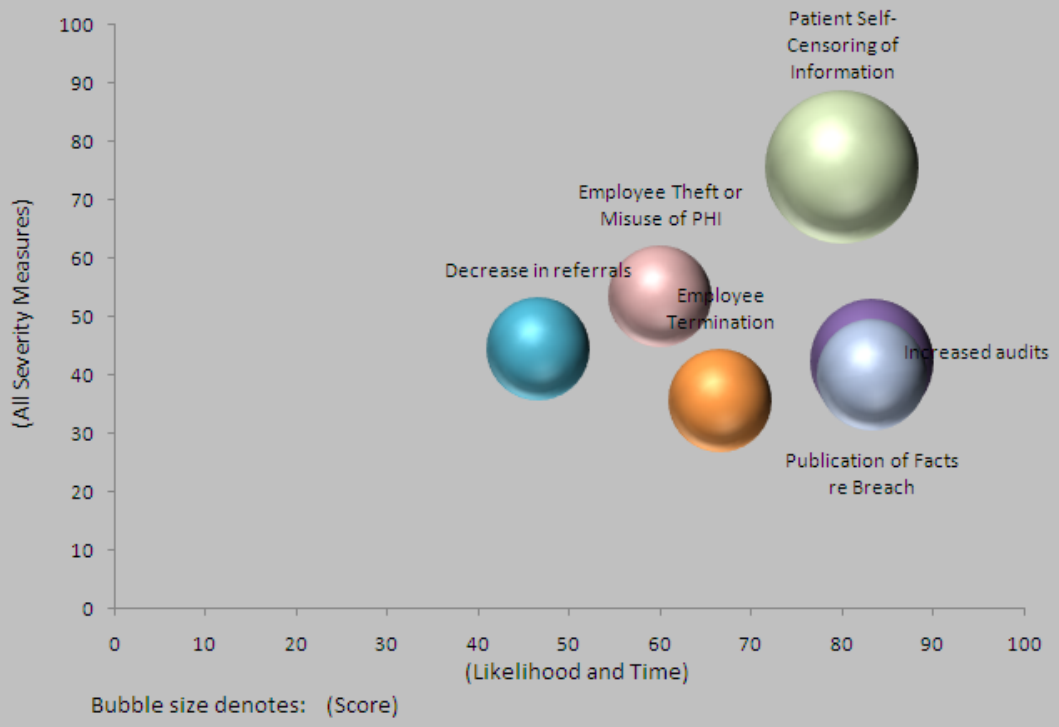
(All Severity Measures)

Horizontal Axis:

(Likelihood and Time)

Bubble Size:

(Score)



Bubble size denotes: (Score)

Lessons Learned

- Enlisting CIO's help was critical in creating an insurance program that would drive improvement
  - CIO helped with insurance policy language
  - CIO leader in "change management"
  - Result: Program offered a carrot and not a stick

Nominee Showcase Presentation

Best Practices

- Developing systemwide security assessment tools with our CISO
- Funded systemwide training through our program savings
- Leveraging our ERM assessment tools to educate

Nominee Showcase Presentation

The Dynamic Duo – CISO Man and Boy Risk!