

# Information Breaches and Security Investments in the Healthcare Sector

Juhee Kwon and M. Eric Johnson  
Center for Digital Strategies  
Tuck School of Business Dartmouth College

**December 12th**  
**WISP 2010 in St. Louis, MO**

# Outline



- # **Research Background**
- # **Research Questions**
- # **Literature Review**
- # **Hypotheses**
- # **Data Collection & Analysis**
- # **Results**
- # **Conclusions**

## # Healthcare IT

- Healthcare IT adoption has resulted in many benefits, but security and privacy risks have increased

## # Healthcare Security

- Shared healthcare information among providers and payers
  - Breaches elsewhere in the network
  - Public good nature by shared information – make less than socially optimal investment
- Healthcare Security Investment is influenced by diverse external sources such as government regulation and public opinion.

# Research Questions



- # **What are the key determinants of security investments: breaches, regulations, or both?**
- # **Is there any difference between the effects of proactive and reactive security investments?**

## ▣ Economic analysis

- Underinvestment in information security
  - While Information sharing provides benefits to each organization and social welfare also increases, each organization will attempt to free ride on the security expenditures of other organizations (Gordon & Loeb, 2002, 2003)
- Appropriate incentive mechanisms are necessary
  - For increases in both organization-level profits and social welfare

## ▣ Game theoretic models

- Strategic interactions between organizations and attackers  
(Cavusoglu, et al., 2008)

## ▣ Cost-benefit analysis

- Return on Security Investment (ROSI) (Karabacak & Sogukpinar, 2005)

- $$ROSI = \frac{(Risk\ exposure * Risk\ mitigated) - Solution\ Cost}{Solution\ Cost}$$

## ▣ Risk–driven security investment

- Fear, uncertainty, and doubt (FUD) drive security expenditures proactively or reactively
- Information breach experience could increase an organization’s fear by exposing its vulnerabilities
  - breach severity and type

		Security Investments
H1a:	<i>Information breach experience</i>	+
H1b:	<i>A type of security breaches</i>	+/-
H1c:	<i># of affected records by a breach</i>	+/-

# Hypotheses

## ▣ Regulation-driven security investment

- Regulations were the most often cited driver affecting organizations' investment strategies
- More than 40 states have adopted breach notification laws since 2002

### Security Investments

H2a: *Breach notification laws*

+

### The Effect of information breach experience on security investment

H2b: *Breach notification laws*

+/-

## ▣ Evaluating Security Investments

- The impact of breaches on investment
  - Reactive actions benefit from learning opportunities
- Due to public-goods nature of security, security investments could generate social benefits in excess of private benefits.

	Breach #
H3a: The drivers of investments	+ / —
H3b: The moderate effect of regulations	—
H3c: Security investments	—

# Data collection



## ▣ **Hospitals : 2,341 hospitals (2005 ~ 2009)**

- The Healthcare Information and Management Systems Society (HIMSS) Analytics™ Database (HADB)
  - Adoption of EMR, size of hospitals, location, academic status, patient composition, for-profit status, and patient volume.

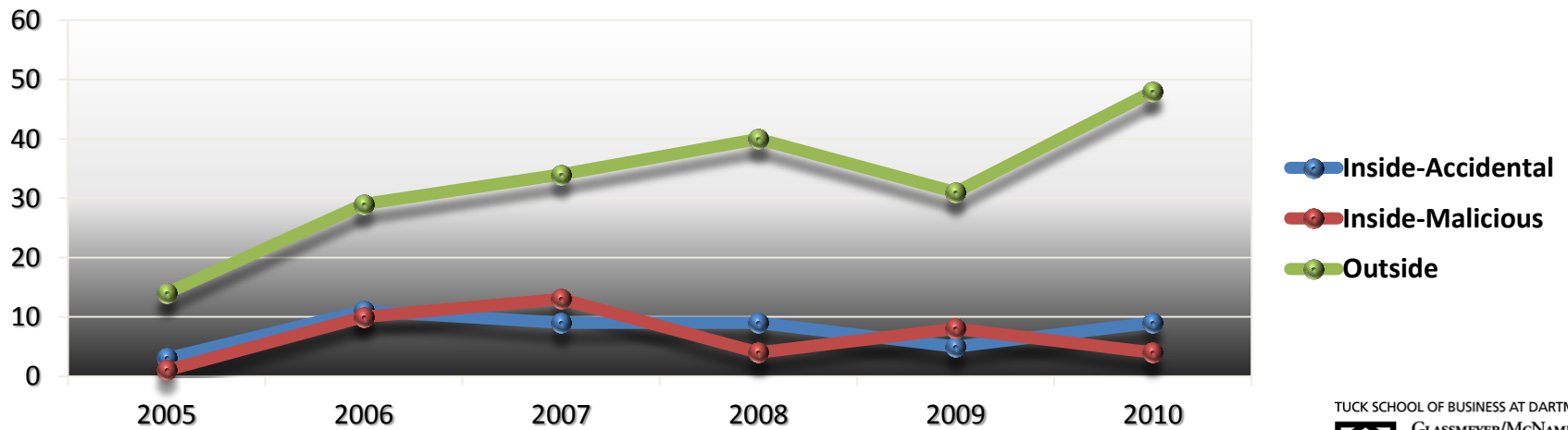
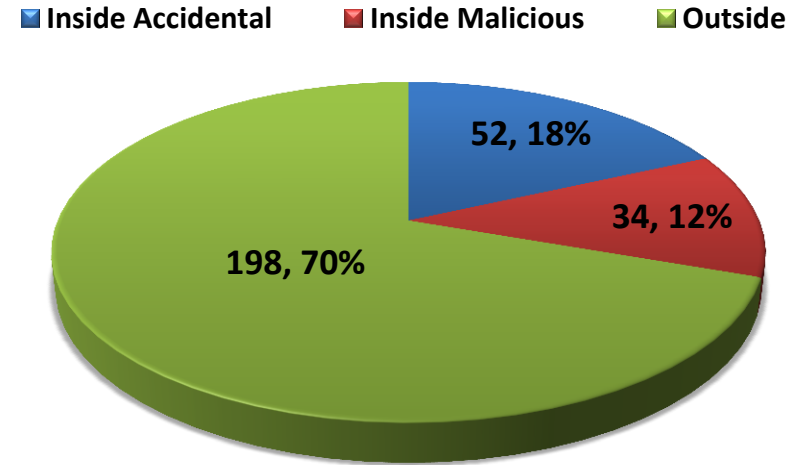
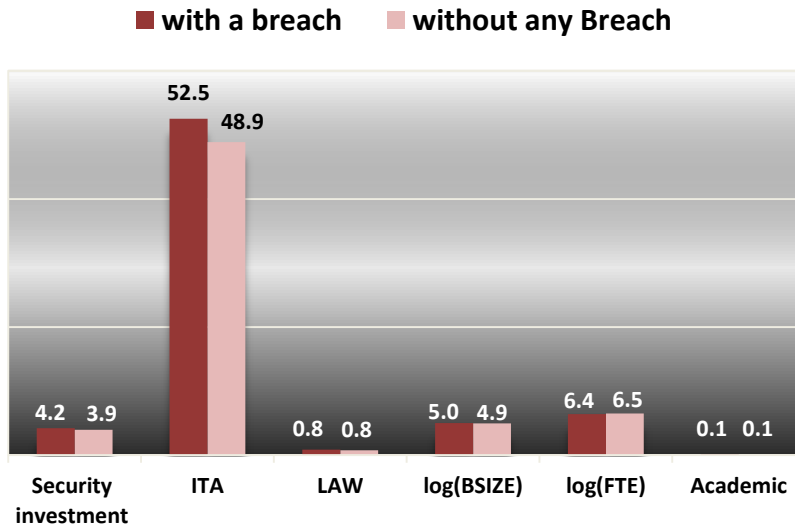
## ▣ **Information Breaches: 274 organizations with breaches**

- Health & Human Services (HHS)
- Identity Theft Resource Center (ITRC)
- Data Loss Database

## ▣ **Breach Notification Laws**

- National Conference of State Legislatures (NCSL)

# Data Collection



# Research Models



Variables	Description	Value
<b>Security investment</b>	# of security applications implemented at different layers	Continuous
<b>BREACH</b>	# of breaches	Continuous
<b>LAW</b>	1 if a state has breach notification laws, otherwise 0	1 or 0
<b>Breach Type</b>	1: <i>Inside-Accidental</i> , 2: <i>Inside- Malicious</i> , and 3: <i>Outside</i>	1,2, or 3
<b>Investment Type</b>	1 if security controls are adopted after a breach, otherwise 0.	1 or 0
<b>Affected Records</b>	# of total records affected by breaches	Continuous
<b>IT App</b>	# of IT applications adopted	Continuous
<b>BSIZE</b>	# of beds	Continuous
<b>FTE</b>	# of Full Time Employees	Continuous
<b>Academic</b>	1 if a hospital is an academic hospital, otherwise 0	1 or 0

## ▣ The effect of breaches and laws on security investments

$$\begin{aligned}
 & \text{SecuritInvestment}_{it} \\
 &= \alpha_0 + \alpha_1 \text{BREACH}_{i,t-\tau} + \alpha_2 \text{BreachType}_{i,t-\tau} + \alpha_3 \text{AffectedRec}_{i,t-\tau} \\
 &+ \alpha_4 \text{LAW}_{i,t} + \alpha_5 (\text{BREACH}_{i,t-\tau} * \text{LAW}_{i,t-\tau}) + \theta_1 \text{ITA}_{it} + \theta_2 \text{BSIZE}_{it} \\
 &+ \theta_3 \text{FTE}_{it} + \theta_4 \text{AC}_{it} + \varepsilon_{1it}
 \end{aligned} \tag{1}$$

## ▣ The effect of breach type on security investments

$$\begin{aligned}
 & \text{SecuritInvestment}_{it} \\
 &= \beta_0 + \beta_1 \text{InsideAcc}_{i,t-\tau} + \beta_2 \text{InsideMal}_{i,t-\tau} + \beta_3 \text{Outside}_{i,t-\tau} \\
 &+ \beta_4 \text{AffectedRec}_{i,t-\tau} + \beta_5 \text{LAW}_{i,t-\tau} + \beta_6 (\text{BREACH}_{i,t-\tau} * \text{LAW}_{i,t-\tau}) \\
 &+ \theta_1 \text{ITA}_{it} + \theta_2 \text{BSIZE}_{it} + \theta_3 \text{FTE}_{it} + \theta_4 \text{AC}_{it} + \varepsilon_{1it}
 \end{aligned} \tag{2}$$

## ▣ The effects of proactive and reactive investment on performance

$$\begin{aligned}
 & \text{BREACH}_{i,t+\tau} \\
 &= \gamma_0 + \gamma_1 \text{SecuritInvestment}_{it} + \gamma_2 \text{Proactive}_{it} + \gamma_3 \text{LAW}_{it} \\
 &+ \gamma_4 (\text{SecuritInvestment}_{it} * \text{Law}_{it}) + \theta_1 \text{ITA}_{it} + \theta_2 \text{BSIZE}_{it} + \theta_3 \text{FTE}_{it} \\
 &+ \theta_4 \text{AC}_{it} + \varepsilon_{2it}
 \end{aligned} \tag{3}$$

( $t$ =year,  $\tau$ =lag time,  $i$ = a hospital)

# Multicollinearity Test

(1) And (2)	Mean	1	2	3	4	5	6	7	8
1.InsideAcc	0.011	1							
2.InsideMal	0.005	-0.007	1						
3.Outside	0.035	<b>0.077</b>	-0.013	1					
4.log(AffectedRec)	2.262	<b>0.246</b>	-0.22	-0.036	1				
5.LAW	0.607	0	<b>0.041</b>	-0.024	-0.11	1			
6.ITA	42.505	-0.021	0.019	0.023	0.239	<b>0.118</b>	1		
7.log(BSIZE)	2.194	0.027	0.03	0.036	<b>0.262</b>	<b>0.141</b>	<b>0.442</b>	1	
8.log(FTE)	2.859	-0.009	0.01	-0.003	<b>0.283</b>	<b>0.124</b>	<b>0.487</b>	<b>0.796</b>	
9.Academic	0.095	0.013	0.024	0.048	<b>0.103</b>	<b>0.074</b>	<b>0.182</b>	<b>0.347</b>	<b>0.416</b>

(3)	Mean	1	2	3	4	5	6
1.Security investment	4.021	1					
2.ProactiveType	0.906	<b>-0.076</b>	1				
3.LAW	0.818	<b>0.079</b>	-0.039	1			
4.ITA	51.693	<b>0.204</b>	-0.02	<b>0.13</b>	1		
5.log(BSIZE)	5.014	<b>0.163</b>	-0.018	<b>0.076</b>	<b>0.552</b>	1	
6.log(FTE)	2.431	<b>0.192</b>	0.002	<b>0.112</b>	<b>0.61</b>	<b>0.784</b>	1
7.Academic	0.089	<b>0.097</b>	-0.023	0.049	<b>0.254</b>	<b>0.355</b>	<b>0.405</b>

# Results



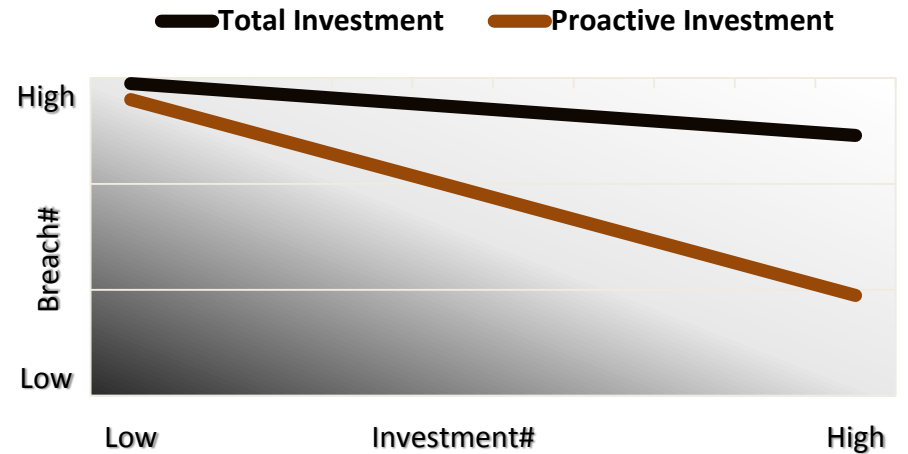
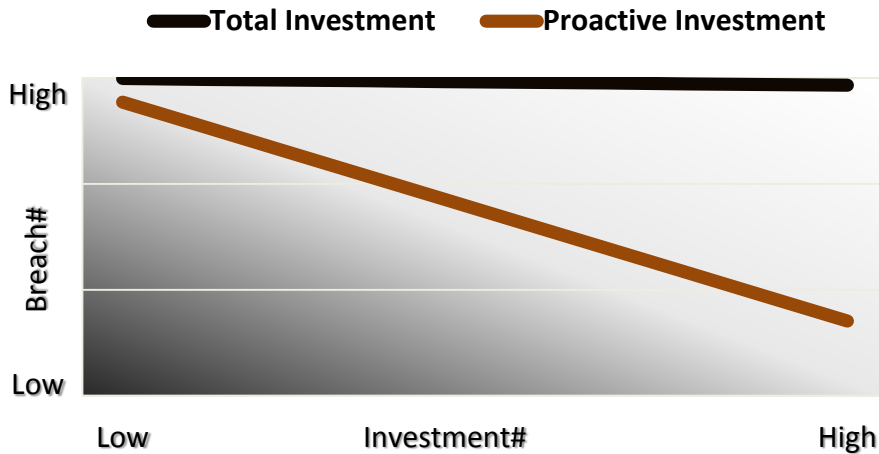
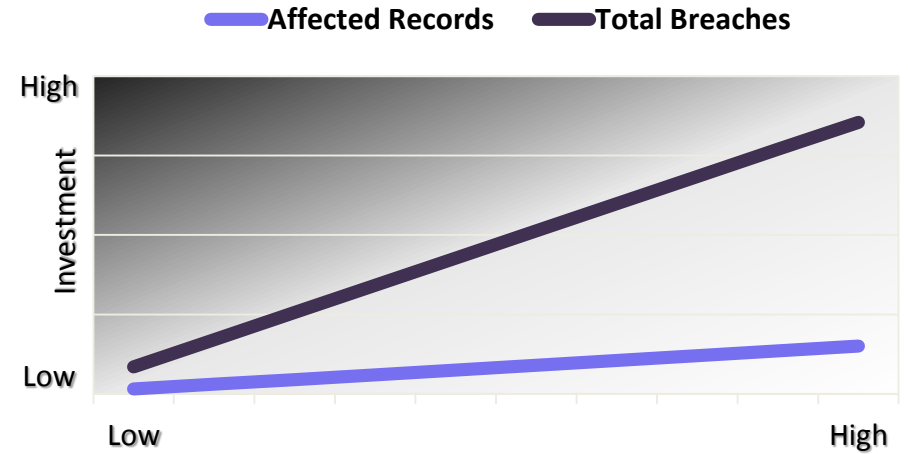
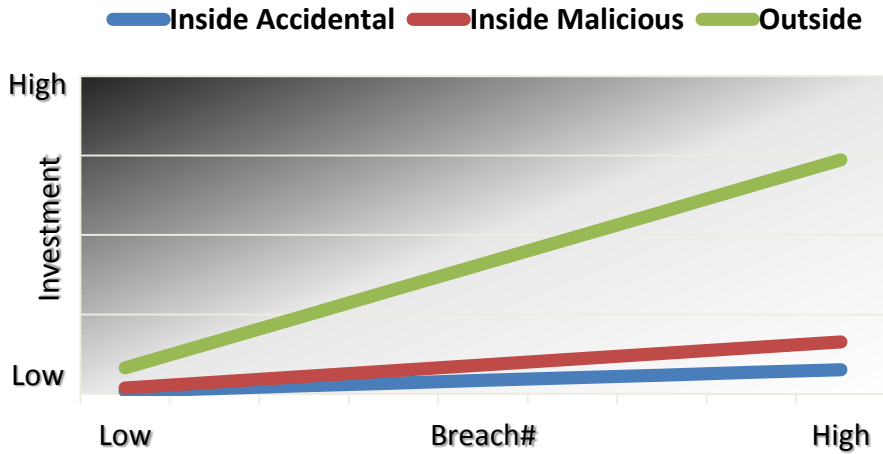
Security Investments			Model(1) and (2)	
<a href="#">H1a:</a>	Information breach experience	+	Supported	1.709** (0.551)
<a href="#">H1b:</a>	Type of security breach	+	Supported	1.694*** (0.310)
	Breaches from outside	+	Supported	1.636*** (0.534)
<a href="#">H1c:</a>	# of affected records by a breach	+	Supported	0.203* (0.111)

Security Investments			Model (1) and (2)	
<a href="#">H2a:</a>	<i>Breach notification laws</i>	+	Not Supported	-1.040 (0.961)
<a href="#">H2b:</a>	<i>The interaction effect of breach notification laws</i>	+	Not Supported	0.556 (0.559)

Breach #		Model (3)		
<a href="#">H3a</a> :	Drivers of investments	—	Supported	-0.109*** (0.010)
<a href="#">H3b</a> :	Moderating effect of regulations	—	Supported	-1.769*** (0.393)
<a href="#">H3c</a> :	Security investments	—	Supported	-0.411*** (0.006)

- ▣ **Breach experience increases security investment**
  - A breach from outside has a larger effect than that from inside.
  - The number of affected records increases security investment.
- ▣ **Proactive investments associated with larger breach reductions (than reactive) at both the organization and state level.**
- ▣ **Breach notification laws significantly enhance the impact of proactive investments at a state-level**

# Results



# Conclusions



- ⌘ **Beach experience motivates security investments, whereas breach notification laws seem to have little influence**
- ⌘ **Proactive investments appear more effective at reducing breaches.**
- ⌘ **Policy makers should focus on encouraging hospitals to proactively invest in security controls rather than imposing penalties for security failures**
- ⌘ **Future Direction**
  - **How security controls collaborate with other security mechanisms such as security policies or security personnel**

# QUESTIONS?

	Model (1)	Model (2)	Model (3)	Model (4)	Hypotheses
	Security Investments		# of Breaches at a hospital	# of Breaches at a state	
Breaches	1.709** (0.551)				<a href="#">H1a</a> : Supported
Breach Type	1.694*** (0.310)				
Inside-Accidental		0.169 (0.630)			<a href="#">H1b</a> : Supported
Inside-Malicious		0.363 (0.673)			
Outside		1.636*** (0.534)			
Affected Record	0.203* (0.111)	0.301* (0.131)			<a href="#">H1c</a> : Supported
LAW	-1.040 (0.961)	-0.859 (0.974)	-0.054* (0.028)	-1.038*** (0.231)	<a href="#">H2a</a> : Not supported
Breach *Law	0.556 (0.559)	-0.465 (0.564)			<a href="#">H2b</a> : Not supported
Security Investments			-0.014** (0.006)	-0.109*** (0.010)	<a href="#">H3a/c</a> : Supported
Security Investments*Law			0.015 (0.028)	-1.769*** (0.393)	<a href="#">H3b</a> : Partially Supported
Proactive Type			-0.459*** (0.008)	-0.411*** (0.006)	<a href="#">H3c</a> : Supported
IT Adoption	0.05 (0.008)	0.004 (0.008)	-0.006** (0.002)	-0.190*** (0.021)	
BSIZE	0.535*** (0.166)	0.477** (0.172)	0.011** (0.004)	4.383*** (1.080)	
FTE	-0.258** (0.095)	-0.220* (0.099)	-0.001 (0.003)	0.077 (0.468)	
Academic	-0.052 (0.402)	-0.163 (0.410)	-0.007 (0.012)	-0.237*** (0.017)	
R-Squares	0.422	0.432	0.394	0.457	

*Notes. Standard errors are in parentheses. p-values are represented by \* Significant at 5%, \*\* Significant at 1%, \*\*\* Significant at 0.1%,*