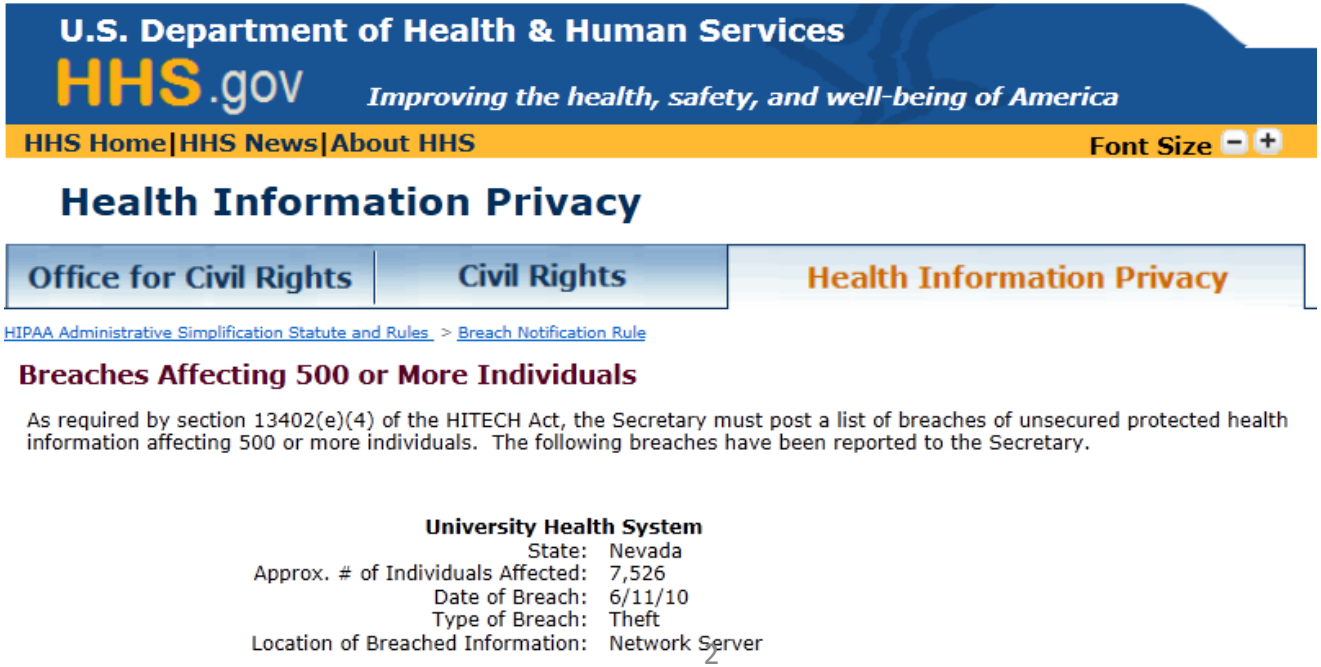
Security Resources, Capabilities and Cultural Values: Links to Security Performance and Regulatory Compliance

WEIS 2012

Juhee Kwon and M. Eric Johnson
Tuck School of Business
Dartmouth College

Healthcare Security Landscape

- **Healthcare data breaches:**
  - 20 ~ 30% of all reported data breaches in 2011.
  - Beach notification rules both in local news outlets and on HHS' website – over 20M impacted patients!



U.S. Department of Health & Human Services

HHS.gov *Improving the health, safety, and well-being of America*

HHS Home | HHS News | About HHS Font Size

Health Information Privacy

Office for Civil Rights | Civil Rights | Health Information Privacy

HIPAA Administrative Simplification Statute and Rules > Breach Notification Rule

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary.

University Health System

State:	Nevada
Approx. # of Individuals Affected:	7,526
Date of Breach:	6/11/10
Type of Breach:	Theft
Location of Breached Information:	Network Server

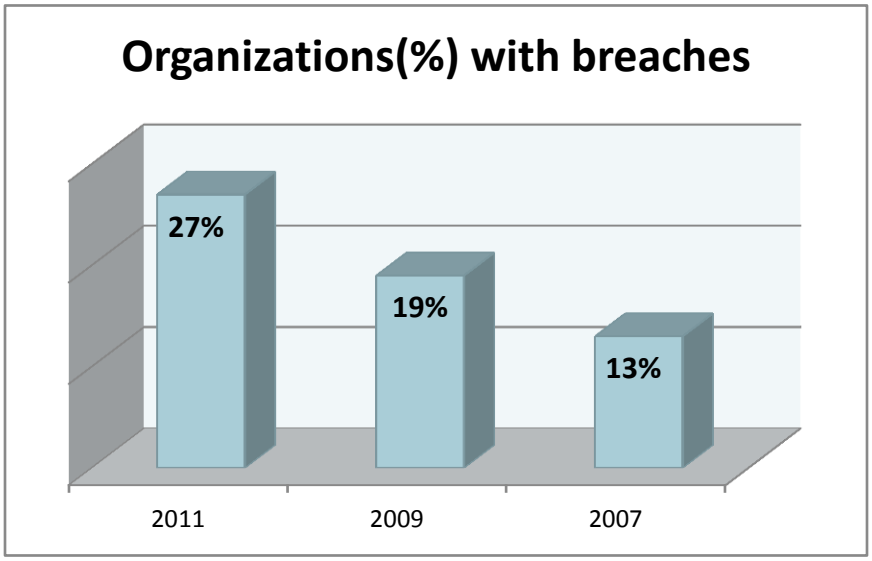
Private Practice

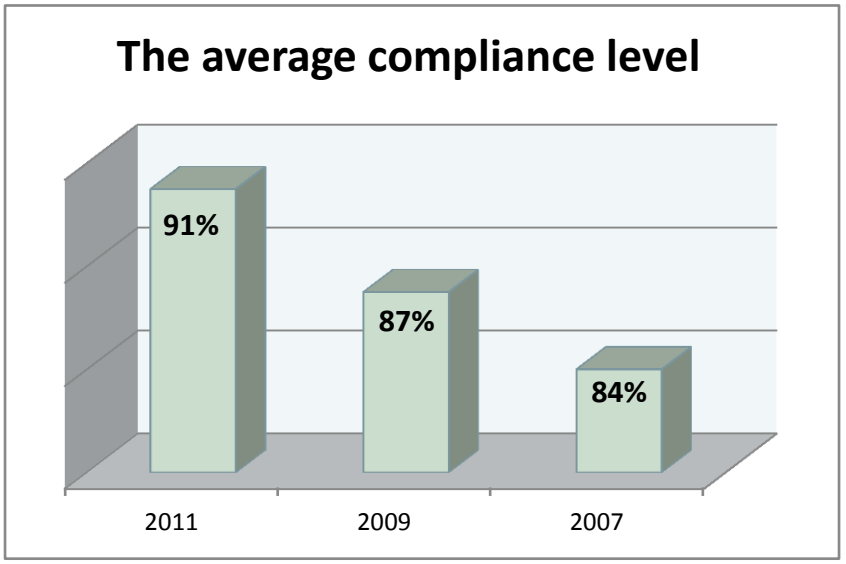
Healthcare Security Landscape

- **Reputational damage and remediation costs**
  - Both data breaches and non-compliance are risks
- **Security goals**
  - Prevent a data breach as well as comply with the evolving regulations
  - Identify, assess, and mitigate risks.
- **Increased adoption of security practices**
  - Security resources and capabilities

Compliance vs. Security Performance

- **Is a "compliant" organization a secure organization?**
- **Maybe not….**
  - Despite high compliance, healthcare data breaches are on the rise according to the 2012 HIMSS Analytics report.





Source: 2012 HIMSS analytics report

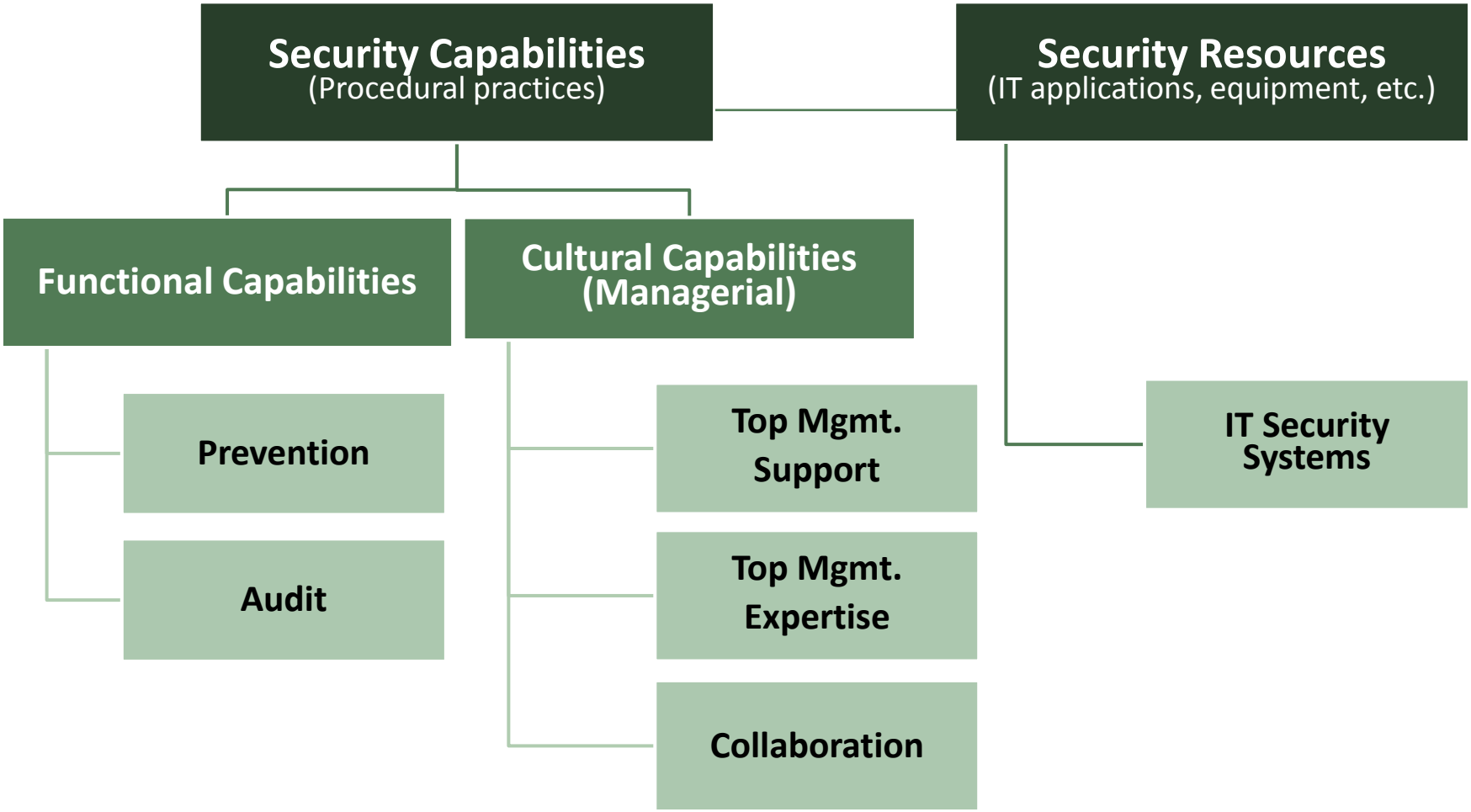
Research Questions

- **How do security resources, functional capabilities, and managerial(cultural) capabilities affect security performance and compliance?**
- **Do security resources and capabilities have any complementary or conflicting effect?**
- **Is compliance associated with breach occurrence?**
  - Compared with other security solutions (i.e., security resources and capabilities).

Theoretical Development

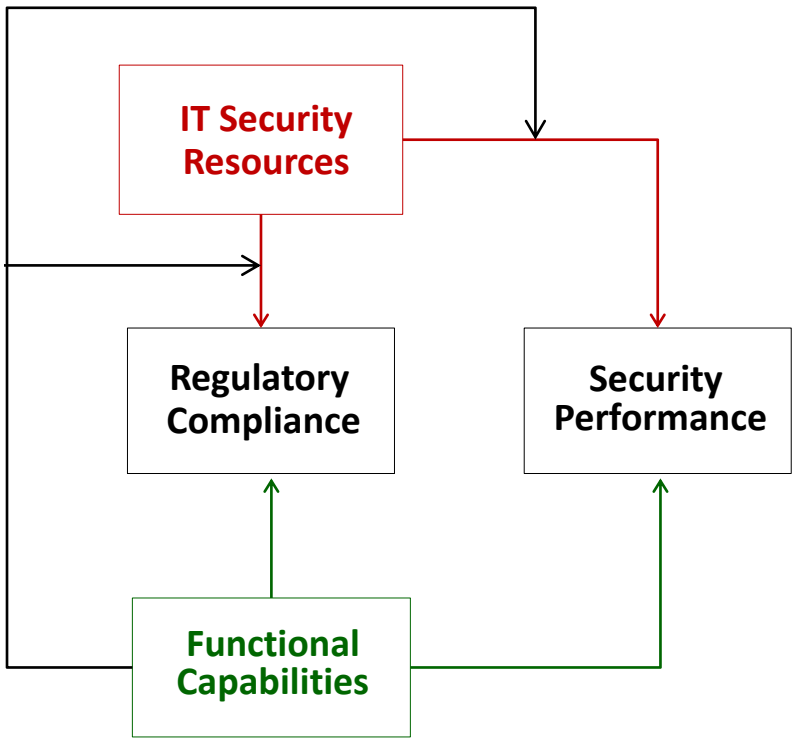
- **The resource-based view (RBV)**
  - Link firm resources and capabilities to organizational performance.
- **What is different in healthcare information security?**
  - More elastic to an organization's reputation than price.
    - Both data breaches and non-compliance are risks
  - Political or regulatory decisions as well as economic, market-based decisions.

The RBV of Information Security



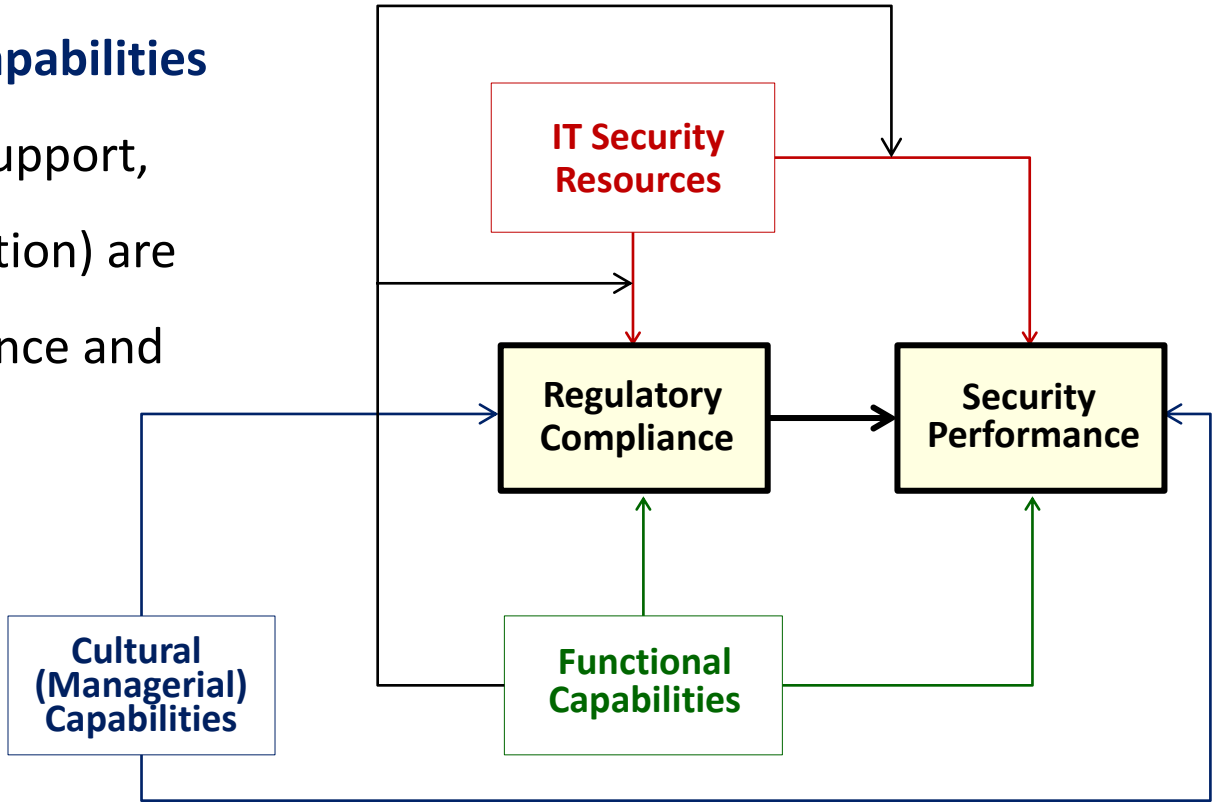
Hypotheses (1)

- **IT security systems** are associated with compliance and security performance.
- **Functional capabilities (prevention and audit)** are associated with compliance and security performance.
- **The interaction between IT security systems and functional (prevention) capabilities** are associated with compliance and security performance.



Hypotheses (2)

- **Cultural (Managerial) capabilities** (i.e., top management support, expertise, and collaboration) are associated with compliance and security performance

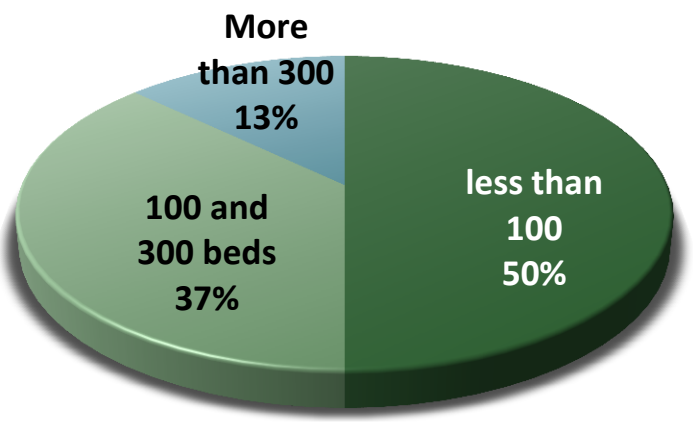


- Higher **regulatory compliance** results in higher **security performance**.

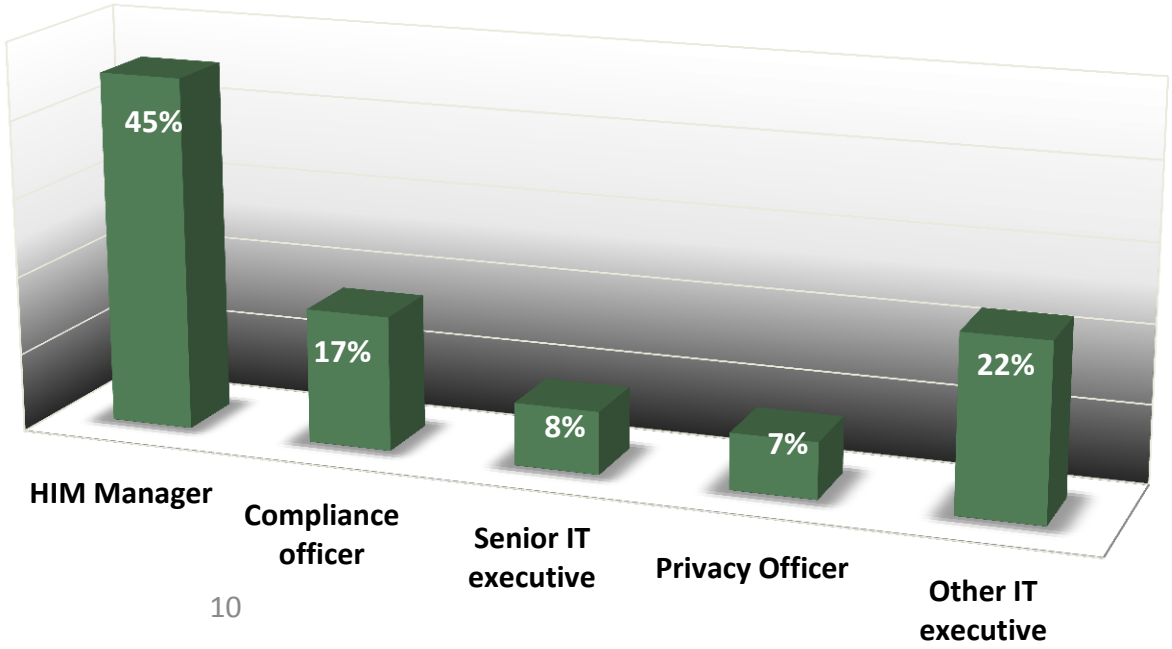
Data Collection

- **The Kroll/HIMMS survey (released in 2010)**
  - Security practices (i.e., IT Systems, policies, and procedures) regarding patient data safety from 250 organizations.

Sizes of Organizations



Types of Respondents



Research Methods

- ***Binomial*** and ***Multinomial*** logit models
  - Breach occurrence and compliance are discrete
  - They do not require any distributional assumption

	Measures	Description
Dependent Variables	**Breach**	Whether a data breach occurred or not
	Compliance	Level of compliance on a seven-point scale
Security Resources	**IT Security systems**	(IT security applications+Physical measures+Data access controls)/3
Functional Capabilities	**Prevention**	(HR+Education+ Data assurance policies)/3
	Audit	(System Audit+Audit policies+Audit log+Regular Audit procedures+Regular review)/5
Cultural (Managerial) Capabilities	**Top Mgmt. Support**	Level of support on a seven-point scale
	Top Mgmt. Expertise	1 if CSO, CPO, or CCO has an ultimate responsibility in security, otherwise 0.
	Collaboration	Level of collaboration on a seven-point scale

Binomial Logit Model

- The relationship between security performance and independent variables
  - $P(security_i = 0|\theta) = \frac{e^{security_i(\theta)}}{1+ e^{security_i(\theta)}}$
  - $security_i = \begin{cases} 0, & no\ data\ breach \\ 1, & otherwise \end{cases}$
  - $security_i(\theta) = \beta_0 + \beta_1 ITSec_i + \beta_2 Prevent_i + \beta_3 Audit_i + \beta_4 (ITSec_i * Prevent_i) + \gamma_1 TopMgmt_i + \gamma_2 Expert_i + \gamma_3 Collabor_i + \delta Compliance_i + \eta_{1-k} \sum_k Controls_k + \varepsilon_i$

Multinomial Logit Model

- The relationship between regulatory compliance and independent variables
  - $P(compliance_i = h|\theta) = \frac{e^{compliance_i(\theta)}}{1+\sum_{h=1}^{M-1} e^{compliance_i(\theta)}}$, h=1,2,…,M
  - $compliance_i = \begin{cases} 1, a\ level\ of\ compliance = 1 \\ 2, a\ level\ of\ complaince = 2 \\ \dots \\ 7, a\ level\ of\ complaicne = 7 \end{cases}$
  - $compliance_i(\theta) = \beta_0 + \beta_1 ITSec_i + \beta_2 Prevent_i + \beta_3 Audit_i + \beta_4 (ITSec_i * Prevent_i) + \gamma_1 TopMgmt_i + \gamma_2 Exper_i + \gamma_3 Collabor_i + \eta_{1-k} \sum_k Controls_k + \varepsilon_i$

Results with Compliance

- **Security resources, functional capabilities, and cultural capabilities are significantly associated with regulatory compliance.**

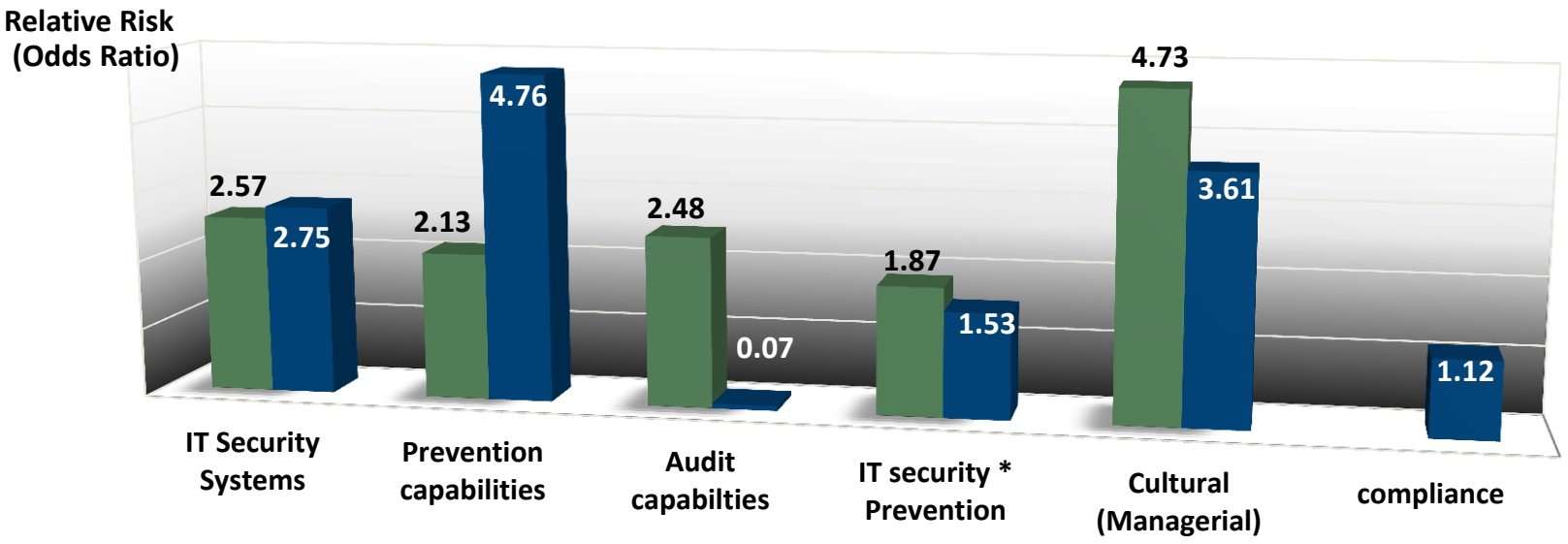
$P(Compliance_i=h\|\theta)$		Main Effects			Interaction Effects		
		Coeff.	StdErr	Odds	Coeff.	StdErr	Odds
IT Security Resources		1.50***	0.51	4.47	0.94*	0.53	2.57
Functional Capabilities	Prevention	0.89***	0.21	2.43	0.75***	0.21	2.13
	Audit	1.11***	0.26	3.04	0.91***	0.27	2.48
IT Resources X Functional Capabilities (Prevention)					0.62***	0.16	1.87
Cultural (Managerial Capabilities)	Top Mgmt. Support	0.19***	0.06	1.21	0.15***	0.06	1.16
	Top Mgmt. Expertise	0.56***	0.13	1.75	0.55***	0.13	1.73
	Collaboration	0.61***	0.07	1.85	0.61***	0.07	1.84
Pseudo R-square				**0.31**			**0.32**

Results with Security Performance

- **Audit capabilities enable an organization detect and report breaches rather than prevent breaches.**

$P(Security_i=0\|\theta)$		Main Effects			Interaction Effects		
		Coeff.	StdErr	Odds	Coeff.	StdErr	Odds
IT Security Systems		1.16***	0.34	3.20	1.01***	0.34	2.75
Functional Capabilities	Prevention	1.62***	0.26	5.03	1.56***	0.26	4.76
	Audit	-2.68***	0.46	0.07	-2.65***	0.45	0.07
IT Resources X Functional Capabilities (Prevention)					0.42**	0.18	1.53
Cultural (Managerial Capabilities)	Top Mgmt. Support	0.16**	0.07	1.17	0.17**	0.07	1.19
	Top Mgmt. Expertise	0.25*	0.16	1.37	0.26*	0.17	1.30
	Collaboration	0.15	0.09	1.13	0.11	0.09	1.12
Compliance		0.27***	0.08	1.31	0.23***	0.08	1.26
Pseudo R-square				**0.15**			**0.17**

Compliance vs. Security Performance



	Compliance	vs.	Security Performance
IT Security Systems	+	<	+
Prevention	+	<	+
IT Security * Prevention	+	>	+
Security Audit	+	>	—
Top Mgmt. Support	+	<	+
Top Mgmt. Expertise	+	>	+
Collaboration	+	>	

Implications

- Balance investments between security resources and related functional capabilities
- Audit capabilities enhance compliance by finding/notifying breaches.
  - Providing incentives for organizations that adopt auditing measures and properly disclose breaches.
- Regulations should provide a framework to encourage a risk-based, as opposed to a static “check the box” list of questions.

THANK YOU